OFICINA INTERNACIONAL DEL TRABAJO

GB.289/7
289.ª reunión

Consejo de Administración

Ginebra, marzo de 2004

SEPTIMO PUNTO DEL ORDEN DEL DIA

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

1. En su 288.ª reunión (noviembre de 2003), el Consejo de Administración pasó a examinar un documento preparado por la Oficina acerca del seguimiento del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003, y de las resoluciones conexas adoptadas por la Oficina Internacional del Trabajo en junio de 2003. En dicho documento [1] la Oficina se refirió a la necesidad de adoptar medidas urgentes en relación con dos aspectos que podrían influir en la decisión de los gobiernos sobre una pronta ratificación del Convenio. Uno de ellos se refiere a la elaboración de una norma mundial interoperable para la «plantilla biométrica basada en una huella dactilar impresa en forma de números en un código de barras» exigida en el Convenio. El pasado mes de noviembre, el Consejo de Administración aprobó un plan propuesto por la Oficina a raíz de una reunión oficiosa mantenida en septiembre de 2003 por expertos gubernamentales, representantes de los armadores y la gente de mar, y de las organizaciones internacionales competentes. Según dicho plan, la Oficina adoptó disposiciones con miras a la preparación «por la vía rápida» de un informe técnico que contenga la norma mundial interoperable indicada, el cual se reproduce en los apéndices al presente documento. Por las razones que se enunciarán más adelante, dicho informe se presenta en dos versiones alternativas: en el apéndice I, una versión referente al perfil biométrico creado a partir de patrones dactilares para los documentos de identidad de la gente de mar, y en el apéndice II, una versión referente al perfil biométrico creado a partir de minucias dactilares para los documentos de identidad de la gente de mar.

2. En el informe técnico se reproduce la norma mundial interoperable preceptuada en el Convenio. Al cumplir la norma recogida en el informe técnico, todos los países que expidan documentos de identidad de la gente de mar (DIM) podrán crear para cada marino una misma plantilla a partir de huellas dactilares e integrarla en un código de barras que se imprimirá en el DIM. Así el marino tendrá, en todos los países que visite, la seguridad de que se podrá leer correctamente el código impreso en su DIM para comprobar su titularidad. La Oficina está en condiciones de garantizar esta interoperabilidad con un grado considerable de certeza, en vista de: *a)* la calidad del informe técnico, *b)* la pericia de

[1] Documento GB.288/3/2.

las personas que supervisaron su preparación y *c)* la idoneidad manifiesta de las distintas medidas previstas en la norma.

3. En lo que respecta a la calidad del informe, la empresa que lo preparó había sido encarecidamente recomendada por un representante gubernamental que participa en la elaboración de la presente norma. Sus dos autoras desempeñaron en dicho gobierno diversas funciones vinculadas a los documentos de identidad y a la biometría. La empresa presta servicios independientes de asesoramiento técnico sobre las tecnologías de autentificación e interviene activamente en la elaboración de las normas internacionales aplicables a los sistemas biométricos, inclusive de las normas que han de ser refrendadas por la Organización Internacional de Normalización (ISO). El informe técnico se preparó en realidad para facilitar una propuesta de suerte que la ISO refrende oportunamente la nueva norma.

4. En lo que respecta a la supervisión, en el informe técnico se toman en cuenta las pautas de orientación y los comentarios facilitados por numerosos representantes gubernamentales expertos, tanto antes de la preparación del informe como durante la misma, y por expertos de la ISO. En particular, la Oficina queda sumamente agradecida por el examen cuidadoso de los proyectos de informe a que procedieron dichos expertos técnicos.

5. La idoneidad de las diversas medidas previstas en la norma se deduce de las referencias claras a sus fundamentos, citadas en el informe técnico. Los primeros corresponden a los requisitos primordiales enunciados en el propio Convenio, que se analizan detenidamente en la sección 5.1 de cada versión del informe técnico presentada en sendos apéndices al presente documento. También fundamentan estas medidas las normas técnicas de la Organización de Aviación Civil Internacional (OACI), que deben acatarse en cumplimiento del Convenio, así como las normas técnicas pertinentes preparadas, o en una fase avanzada de elaboración, en el marco de la ISO. La creatividad del informe técnico reside pues esencialmente en la configuración de un cuerpo normativo uniforme a partir de toda una serie de procedimientos técnicos ya existentes y que resultan ser, sin duda, los más adecuados para realizar las funciones exigidas por la norma.

6. Hubo sin embargo un aspecto que suscitó fuertes divergencias entre los expertos consultados, esto es, la manera de convertir la imagen de una huella dactilar en una serie numérica inscrita en una plantilla para su representación en un código de barras. Se preconizan para ello dos métodos, contemplados en unas normas que la ISO está perfilando: el método basado en la utilización de *patrones*, en el cual la plantilla se crea a partir de patrones geométricos conformados por crestas y surcos dactilares, y el método basado en la utilización de *minucias*, en que el contenido de la plantilla se configura a partir del número y la posición de las minucias (puntos de terminación y puntos de bifurcación) ubicadas en dichas crestas dactilares. Ante estas dos opciones, en diciembre de 2003 la Oficina cursó una solicitud de información a los gobiernos de todos los Estados Miembros de la OIT, y remitió un cuestionario a los proveedores más conocidos de tecnología y dispositivos apropiados a estos efectos. Entre las respuestas recibidas de los gobiernos al 11 de febrero de 2004, 28 versaban sobre la pregunta específica relativa a la tecnología. En 12 de ellas (entre las cuales figuraban las de dos grandes países proveedores de mano de obra) se expresaba preferencia por las plantillas creadas a partir de *minucias*, mientras que en 13 no se manifestaba preferencia por tecnología alguna, y en tres se expresaba predilección por el método basado en la utilización de *patrones.*

7. Para superar este dilema, en el presente informe técnico se exponen las dos versiones alternativas: la primera (ILO SID-0001) versa sobre la tecnología basada en la utilización de *patrones* (apéndice I), mientras que la segunda (ILO SID-0002) versa sobre la utilización de la tecnología basada en *minucias* (apéndice II). En la sección 5.1.4 de cada versión se explica respectivamente por qué la tecnología basada en *patrones* resulta

preferible respecto a aquella basada en *minucias* (ILO SID-0001), y por qué el sistema basado en *minucias* puede resultar más ventajoso que aquel basado en *patrones* (ILO SID-0002). Por las razones que se enuncian a continuación, resulta claro que el método basado en la utilización de *patrones*, que en realidad fue el que se recomendó en la reunión de septiembre de 2003, mencionada en el párrafo 1, atendería mejor a los requisitos contemplados en el Convenio. Sin embargo, el método basado en *minucias* tiene la ventaja de que los gobiernos están más familiarizados con su utilización y de que encierra un gran potencial de integración con los demás sistemas nacionales en que se utiliza tecnología basada en el empleo de huellas dactilares, especialmente en la investigación de los delitos.

8. Desde un punto de vista técnico, ambos métodos resultan muy adecuados para verificar de modo interoperable y eficaz si el portador del documento de identidad es el marino titular del mismo. Existe con todo cierto margen de incertidumbre respecto al cumplimiento de una función necesaria para la comprobación de los DIM en que se almacenan *minucias*: el código de barras sólo tiene cabida para almacenar una cantidad limitada de información. Los expertos suelen coincidir en que la información debería referirse a dos huellas dactilares (de forma que si en el momento de la verificación no estuviera disponible un dedo o la imagen correspondiente no resultase bastante clara, se pudiese recurrir a la huella de otro dedo). En cambio, cuando se utilice el método basado en *patrones*, la información que se recabe con arreglo a las normas vigentes tendrá siempre cabida en el código de barras. Por otra parte, cabe que cuando se siga el método basado en la utilización de *minucias*, algunas de ellas exijan más información que la que pueda almacenarse en el código de barras. La solución más sencilla en estos casos consistiría en reducir el número de *minucias* que deban tomarse en consideración, según se indica en el documento ILO SID-0002 (véase la sección 5.1.3, segundo párrafo). Conviene tener presente sin embargo que, al no existir para esta operación de «truncamiento» una norma de probada eficacia, todavía no cabe garantizar a ciencia cierta que siempre se obtendrá la misma plantilla.

9. En líneas más generales cabe pues afirmar que el método basado en la utilización de *patrones* brinda por ahora mayor grado de fiabilidad. Las normas internacionales referentes a ambos métodos están todavía en fase de proyecto (aunque adelantada). Terceros independientes han probado oficialmente la eficacia de ciertos productos que se ajustan al proyecto de norma basado en la utilización de *patrones*, pero no los productos que en principio se ajustan al proyecto de norma basado en el empleo de *minucias*. Según se indicó en algunas respuestas al cuestionario enviado a los proveedores, cuando se haya terminado de elaborar la norma internacional y su clientela solicite productos ajustados a la norma, los vendedores de productos basados en la utilización de *minucias* podrían introducir los cambios necesarios. Ahora bien, como suele suceder siempre que se actualiza tecnología de este tipo, será preciso someter los productos basados en la utilización de *minucias* (inclusive los efectos del truncamiento necesario para la inclusión de los datos en la plantilla del DIM) a una prueba independiente a fin de garantizar que los cambios introducidos no mermarán la eficacia de los productos o no generarán en ellos deficiencias imprevistas.

10. En virtud del apartado *c)* del párrafo 8 del artículo 3 del Convenio, se exige que «el material necesario para proveer y verificar los datos biométricos sea ..., en general, asequible para los gobiernos a bajo coste». A este respecto, el método basado en la utilización de *patrones* resulta ser ligeramente preferible, ya que podría funcionar eficazmente con una imagen de menor resolución que la necesaria para el otro método. Se podría utilizar así un material menos costoso para la adquisición de la imagen de la huella dactilar durante la expedición de los DIM y la subsiguiente verificación de la identidad del portador. Con todo, un gobierno respondió que en este caso convendría utilizar sensores ópticos, aunque son más onerosos (y no son indispensables para aplicar el método biométrico basado en *patrones*) por resultar el material necesario más resistente en entornos marítimos. Otro factor que podría incidir en el coste del material estriba en que,

pese a haber varios consultores, integradores de sistemas y otros fabricantes de material conocidos que utilizan una tecnología basada en *patrones*, son muchos más los proveedores de tecnología basada en la utilización de *minucias* que tienen a sus propios consultores, integradores de sistemas, y otros fabricantes de material. Sin embargo, hasta tanto una prueba oficial e independiente de los productos venga a demostrar que éstos cumplen (o aplican) efectivamente el proyecto de norma internacional, es posible que los compradores de material basado en *minucias* se vean obligados a depender de un número reducido de proveedores (quizás de uno solo).

11. El método basado en la utilización de *minucias* presenta sin duda una deficiencia en relación con el requisito según el cual «no podrán reconstituirse datos [biométricos] a partir de la plantilla» (apartado *b)* del párrafo 8 del artículo 3). Se sabe en efecto de métodos para elaborar dispositivos que permitirían falsificar datos de las huellas dactilares con la ayuda de una plantilla creada a partir de *minucias.* En cambio, no se sabe de ningún método basado en el empleo de *patrones* que presente este riesgo.

12. Los gobiernos que se doten de sistemas basados en la utilización de *minucias* no deberían tener dificultades especiales en aplicar programas basados en la utilización de *patrones* para producir y verificar la plantilla de una huella dactilar (ya que es posible hacer funcionar eficazmente en un mismo ordenador varios programas completamente distintos). Sin embargo, no sería posible emplear una plantilla creada a partir de *patrones* para efectuar búsquedas en bases de datos donde las huellas dactilares estén almacenadas solamente en plantillas creadas a partir de *minucias*, especialmente en las bases nacionales de datos de investigación penal. Debe quedar claro que la utilización de plantillas con fines distintos de la verificación de la identidad de los marinos no se ajusta sin embargo a la finalidad del Convenio, según se recoge en varias disposiciones de este último, como por ejemplo el párrafo 7 del artículo 4, en cuya virtud: «los Miembros velarán por que los datos personales registrados en la base electrónica de datos no se utilicen a efectos distintos de la verificación de los documentos de identidad de la gente de mar».

13. Sin querer por tanto menospreciar las virtudes del método basado en la utilización de *minucias*, la Oficina concluye en general que convendría adoptar el método basado en el empleo de *patrones* por ser la solución que mejor cumple los requisitos y los objetivos del Convenio sobre los documentos de identidad de la gente de mar. Valga especificar a este respecto que el Convenio no tiene por objeto la adopción de la mejor solución posible; ya se decidió expresamente no incorporar la solución más eficaz, consistente en utilizar una imagen biométrica almacenada en un microprocesador. De lo que se trata es esencialmente de llegar a una solución biométrica que sea relativamente económica y aceptable, que pueda utilizarse adecuadamente más allá de los cinco o diez primeros años de vigencia del Convenio, que sirva de complemento eficaz para los demás datos personales exigidos en el Convenio, como la firma y la fotografía, y de que esta solución única se ponga en práctica con carácter urgente. Aunque todavía debe comprobarse en un laboratorio de certificación la eficacia de la norma expuesta en el presente informe [2], se sugiere que el Consejo de Administración tenga a bien dar ahora su aprobación. Ello permitiría a los Miembros que se planteen ratificar el Convenio hacerse una idea clara de los requisitos señalados al respecto. Los detalles que eventualmente necesiten mayor ajuste podrían perfilarse más adelante.

[2] Véase documento GB.288/3/2, párrafo 8.

14. ***En vista de cuanto antecede, el Consejo de Administración quizá estime oportuno:***

a) seleccionar la opción basada en la utilización de patrones, recomendada por la Oficina, y aprobar el documento ILO SID-0001 (apéndice I al presente documento), en que se presenta la norma aplicable a la plantilla de huellas dactilares exigida en virtud del apartado k) del anexo I al Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003, o bien,

b) seleccionar la opción basada en minucias y aprobar el documento ILO SID-0002 (apéndice II al presente documento), en que se presenta la norma aplicable a la plantilla de huellas dactilares exigida en virtud del apartado k) del anexo I al Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003.

Ginebra, 24 de febrero de 2004.

Punto que requiere decisión: párrafo 14.

Apéndice I

Perfil biométrico creado a partir de patrones dactilares para los documentos de identidad de la gente de mar

Editores: Cynthia L. Musselman
cynthia@authenti-corp.com
teléfono: 540 837 2450

Valorie S. Valencia
valorie@authenti-corp.com
teléfono: 480 889 6444

Indice

Prólogo

La Organización Internacional del Trabajo, constituida en 1919, es un organismo especializado de las Naciones Unidas (NU) de carácter tripartito, en el que participan en pie de igualdad representantes de los gobiernos, de los empleadores y de los trabajadores. En junio de 2003 la OIT adoptó el Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185). La revisión del antiguo convenio, de 1958, fue motivada por una serie de debates celebrados en la Organización Marítima Internacional (OMI) y obedecía a la necesidad de reconsiderar las medidas y los procedimientos encaminados a prevenir y evitar los actos de terrorismo que amenazan la seguridad de los buques, de sus pasajeros y de sus tripulantes. Se ha puesto el nuevo convenio de la OIT en conocimiento de los gobiernos de los Estados Miembros de dicha organización a fin de que lo estudien con miras a su ratificación. Al ser un tratado internacional, cobrará carácter vinculante para todos los Miembros que lo ratifiquen.

La Oficina Internacional del Trabajo (secretaría de la Organización) encargó a las autoras del presente documento que preparasen un proyecto de informe técnico para fundamentar la elaboración de una norma que se someterá a la Organización Internacional de Normalización (ISO) con miras a su refrendo, para la adopción de una plantilla biométrica interoperable con arreglo a lo preceptuado en el Convenio núm. 185. Esta norma será aplicable a la adquisición de los datos correspondientes a las huellas dactilares, a la generación de plantillas y al almacenamiento en códigos de barras. El informe debía versar sobre las tecnologías de impresión y de lectura más apropiadas, así como sobre los procedimientos de registro, el formato del código de barras, los captores/lectores de los datos biométricos, y las consideraciones relativas a las bases de datos y al formato de una plantilla biométrica interoperable en el mundo entero. En el informe también debían tomarse en cuenta la calidad y la interoperabilidad de las bases de datos.

La ISO y la Comisión Electrotécnica Internacional (IEC) conforman el sistema especializado de normalización mundial. Las entidades nacionales que son miembros de la ISO o de la IEC participan en la elaboración de normas internacionales a través de unas comisiones técnicas constituidas por cada entidad competente para tratar de ámbitos específicos de actividad técnica. Las comisiones técnicas de la ISO y de la IEC colaboran en campos que para ellas revisten un interés mutuo. También participan en esta labor otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con la ISO y la IEC.

Las normas internacionales se redactan atendiendo a las reglas sentadas en la parte 2 del documento ISO/IEC sobre directrices.

En lo que respecta a las tecnologías de la información, la ISO y la IEC han constituido una comisión técnica mixta, denominada ISO/IEC JTC 1. Los proyectos de normas internacionales adoptados por esta comisión técnica mixta se distribuyen a los órganos nacionales competentes para que los sometan a votación.

El presente informe técnico fue preparado por la Oficina Internacional del Trabajo (OIT) y puede someterse a guisa de contribución técnica a la ISO/IEC JTC 1 SC37 en materia de biometría.

El presente informe, ILO SID-0001, titulado *Perfil biométrico creado a partir de patrones dactilares para los documentos de identidad de la gente de mar*, se estructura en cinco secciones, a saber:

- *Sección 1 – Ambito de aplicación*
- *Sección 2 – Cumplimiento*
- *Sección 3 – Referencias*
- *Sección 4 – Definiciones*
- *Sección 5 – Requisitos biométricos aplicables a los documentos de identidad de la gente de mar*

La sección 5, relativa a los requisitos biométricos aplicables a los documentos de identidad de la gente de mar, se subdivide a su vez en cinco apartados, a saber:

- *Sección 5.1 – Requisitos biométricos aplicables a los documentos de identidad de la gente de mar creados a partir de patrones dactilares*

- *Sección 5.2 – Requisitos aplicables al código de barras de los documentos de identidad de la gente de mar y a los lectores de estos códigos*
- *Sección 5.3 – Requisitos aplicables a la verificación de los datos biométricos en los documentos de identidad de la gente de mar*
- *Sección 5.4 – Requisitos aplicables a la base de datos de los documentos de identidad de la gente de mar*

0. Introducción

0.1. Motivos de la elaboración del documento

La Organización Internacional del Trabajo, constituida en 1919, es un organismo especializado de las Naciones Unidas (NU), con estructura tripartita, en que participan en pie de igualdad representantes de los gobiernos, de los empleadores y de los trabajadores. Tras los ataques terroristas del 11 de septiembre de 2001, la Organización Internacional del Trabajo hizo lo propio para que se revisase mediante un procedimiento acelerado el Convenio sobre los documentos de identidad de la gente de mar de 1958. El nuevo instrumento resultante, o sea, el Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185), adoptado en la reunión de la Conferencia Internacional del Trabajo de junio de 2003, permitió introducir en los documentos de identidad de la gente de mar (o «DIM») dispositivos de seguridad modernos destinados a paliar con carácter urgente el riesgo de que la gente de mar no sea admitida en el territorio de los países en que atracan sus buques con miras al disfrute de un permiso para bajar a tierra, tránsito o reembarco en otro buque. Uno de estos dispositivos de seguridad es la plantilla biométrica creada a partir de huellas dactilares, que revestirá la forma de una serie numérica impresa en un código de barras PDF417 «acorde con una norma que se elaborará posteriormente» (Convenio núm. 185, anexo I).

En una resolución adoptada por la Conferencia Internacional del Trabajo en su reunión de junio de 2003, se pidió al Director General de la OIT que adoptase medidas urgentes «con miras a la elaboración por las instituciones competentes de una norma mundial interoperable» para la plantilla biométrica antes mencionada, especialmente en colaboración con la Organización de Aviación Civil Internacional (OACI). En una reunión celebrada en la OIT en septiembre de 2003, a la que asistieron representantes de gobiernos, armadores y gente de mar, así como de la OACI y la ISO, resultó claro que la OACI, que recomendaba una solución de reconocimiento biométrico diferente (véase más adelante) para determinar la norma aplicable a los pasaportes de lectura mecánica, no estaba en condiciones de participar activamente en la elaboración de la plantilla exigida para el nuevo DIM. También se tomó nota de que la urgencia de poner en práctica el Convenio núm. 185 obligaba a descartar la utilización de los procedimientos ordinarios para elaborar dicha plantilla en el marco de la Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC).

En consecuencia, la Oficina Internacional del Trabajo encargó el presente informe técnico y pidió que en él se reflejasen las exigencias contempladas en el Convenio de 2003 sobre los documentos de identidad de la gente de mar, en el cual se recogen unos requisitos rigurosos para la identificación personal de la gente de mar a partir de información biométrica a escala internacional. Los autores del presente informe técnico, ILO SID-0001 Rev. 05, las autoras presentan un perfil biométrico a fin de que sirva la norma para la generación y el almacenamiento de plantillas de huellas dactilares creadas a partir de patrones biométricos en un código de barras PDF417 que se imprimirá en la próxima generación de DIM, y en las bases electrónicas de datos nacionales de los Miembros (Convenio Internacional del Trabajo núm. 185, anexo I y anexo II, respectivamente). Este perfil biométrico se estructura una forma casi ajustada a las normas ISO; podría materializarse en una norma, e incluso, con el tiempo, en un documento de adquisición una vez que los requisitos aplicables se hayan examinado y armonizado a escala internacional.

0.2. Esfuerzos conexos

En los últimos años se han realizado varios estudios, experimentos, programas piloto y productos a fin de acelerar la inspección en los puestos fronterizos. En este empeño se procurará en gran medida incorporar tecnología de reconocimiento biométrico a la próxima generación de documentos de viaje y de documentos de identidad internacionales. Al elaborar y aprobar el

Convenio núm. 185, la Organización Internacional del Trabajo cuidó de definir los requisitos aplicables a la próxima generación de DIM, en los que se integrarán los datos biométricos de identidad de cada marino (titular del documento) y en los que se almacenarán las plantillas biométricas en un código de barras.

Antes del 11 de septiembre de 2001, el sector de la biometría ya había emprendido varios proyectos de producción de normas para facilitar la elaboración de productos y sistemas interoperables de reconocimiento biométrico, así como el intercambio de datos biométricos entre productos y sistemas, y requisitos para garantizar la integridad y la confidencialidad de los datos biométricos.

- ISO/IEC FCD 19784 – tecnologías de la información – interfaz de programación de aplicación de la biometría (BioAPI) (ISO/IEC JTC 1 SC37 N, núm. 55 [1], de 17 de diciembre de 2002), en el que se presenta un interfaz de programación de aplicación que garantiza que los productos y los sistemas conformes son interoperables entre sí. (También es una norma del Instituto Nacional de Normas Estadounidense/Comisión Internacional para las Normas relativas a las Tecnologías de la Información: ANSI/INCITS 358:2002 – tecnologías de la información – especificación BioAPI.)
- ISO/IEC CD 19785 – tecnologías de la información – marco común para los formatos de intercambio de datos biométricos (CBEFF) (ISO/IEC JTC 1 SC37 N 208, de 14 de julio de 2003).
- ISO/IEC WD 19794-3 – formatos de intercambio de datos biométricos – parte 3: datos correspondientes a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003). (También se trata de una norma ANSI/INCITS: ANSI/INCITS 377 – formato de intercambio de información basada en patrones dactilares.)
- Norma de la Organización de Aviación Civil Internacional (OACI) sobre los documentos de viaje de lectura mecánica, encargada por la ISO/IEC JTC1 SC17.

  NB: La OACI recomendó últimamente que en la próxima generación de documentos de viaje se integre una tecnología sin contacto para tarjetas inteligentes, así como una o varias indicaciones biométricas (en virtud de la norma de la OACI sobre documentos de viaje de lectura mecánica se exigen datos biométricos faciales, y también podrían incorporarse sistemas de reconocimiento de huellas dactilares o del iris). Aunque los documentos previstos por la OIT para la gente de mar son documentos de identidad (y no documentos de viaje), la OIT procurará ajustarse en la medida de lo posible a la norma propuesta por la OACI para la próxima generación de documentos de viaje oficiales de lectura mecánica. Resulta importante destacar que en la próxima generación de DIM prevista por la OIT, los datos biométricos se almacenarán en un código de barras (en vez de en un circuito integrado, como se prevé en la norma recomendada de la OACI para los documentos de viaje de lectura mecánica). Esta diferencia tiene hondas repercusiones en el perfil biométrico del DIM, pues si bien por un lado el almacenamiento en un código de barras resulta más económico que en un circuito integrado, por otro lado la capacidad de almacenamiento es mucho menor en el código de barras PDF417 para DIM que en el circuito integrado recomendado por la OACI.

En vista de que en la próxima generación de DIM prevista por la OIT se utilizará tecnología con códigos de barras para almacenar la información biométrica y contribuir así al cumplimiento de los requisitos previstos por la OIT con miras a la interoperabilidad internacional de los DIM, este perfil biométrico determina el formato de almacenamiento de las plantillas de huellas dactilares en el código de barras PDF417. En consecuencia, las normas ISO/IEC 15438:2001 (símbolos de los códigos de barras PDF417) e ISO/IEC FDIS 15415 (calidad de impresión de los símbolos del código de barras PDF417) son fundamentalmente aplicables a este perfil biométrico.

Combinadas, las normas ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC WD 19794-3 – formatos de intercambio de datos biométricos – parte 3: datos relativos a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003), y el documento 9303 de la OACI, son la base sobre la cual se desarrollará el potencial biométrico de los sistemas aplicables a los DIM. Al propio tiempo, se han elaborado otras normas (como ANSI/INCITS 358:2002 – tecnologías de la información – especificación BioAPI), o se están elaborando, como la norma ISO/IEC WD 19794-4 –

[1] Para averiguar el número del documento mencionado, es decir, del documento ISO/IEC JTC 1 SC37, véase en el sitio Web *www.jtcl.org,* seleccionar subcomisión 37, buscar los documentos e introducir el número del documento en el campo «N».

formatos de intercambios de datos biométricos – parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003), que resultarán pertinentes según se indica más adelante.

0.3. Determinación de la tecnología biométrica idónea para almacenar las huellas dactilares en los documentos de identidad de la gente de mar

En el Convenio núm. 185 de la OIT se requiere que los DIM sean interoperables a escala internacional. La OIT se ve por tanto obligada a optar, respecto a la próxima generación de DIM, entre almacenar datos biométricos correspondientes a *imágenes* dactilares, a *minucias* de los dedos o a puntos característicos *(patrones)* de los mismos. Para fundamentar su decisión, la OIT encargó la elaboración de dos informes técnicos y se realizó una encuesta entre los Miembros de la OIT y las comunidades técnicas consultadas. En este informe, ILO SID-0001, se presentan los requisitos técnicos que se aplicarían si se adoptase la tecnología de reconocimiento biométrico basada en *patrones dactilares*, que se ha considerado la solución más acorde con los requisitos de aplicación para los DIM sentados por la OIT con arreglo a los requisitos señalados en la sección 5.1.4 del presente informe, relativa a las *Plantillas de las huellas dactilares*.

La OIT se reserva sin embargo el derecho de reconsiderar esta decisión, toda vez que las normas internacionales maduran y las opciones tecnológicas evolucionan, lo cual también coadyuva al cumplimiento en beneficio del Convenio núm. 185 de la OIT.

1. Ambito de aplicación

En la presente versión del informe técnico (ILO SID-0001), titulada *Perfil biométrico creado a partir de patrones dactilares para los documentos de identidad de la gente de mar,* se facilitan pautas de orientación para incorporar a los DIM la tecnología de reconocimiento biométrico basado en patrones dactilares, con arreglo al Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185). Las autoras del presente documento se inspiraron también en otras fuentes, a saber: 1) las notas informativas referentes a las plantillas biométricas, preparadas en la reunión oficiosa sobre la biometría al servicio de los documentos de identidad de la gente de mar, celebrada los días 29 y 30 de septiembre de 2003; 2) material de apoyo adicional; 3) la reunión de consulta técnica mantenida en Ginebra del 5 al 7 de diciembre de 2003, y 4) asesoramiento de expertos en este ámbito.

La biometría servirá para incrementar el potencial de vinculación entre los DIM y sus titulares.

El presente informe se estructura de la siguiente manera: en la sección 2 se determinan los requisitos de cumplimiento correspondientes a este perfil biométrico. En las secciones 3 y 4 se presentan respectivamente las referencias técnicas y las definiciones útiles para la lectura del presente documento. En la sección 5 se recogen los requisitos biométricos que deben reunir los DIM. Esta última sección se subdivide a su vez en cuatro apartados, a saber:

- Sección 5.1 – *Requisitos biométricos aplicables a los documentos de identidad de la gente de mar creados a partir de patrones dactilares*, relativos al registro de las huellas dactilares, a su adquisición y al formato de la plantilla en que éstas han de recogerse en la próxima generación de documentos de identidad de la gente de mar.
- Sección 5.2 – *Requisitos aplicables al código de barras de los documentos de identidad de la gente de mar y al lector de este código*, es decir en relación con el formato del código de barras, la tecnología y las especificaciones de impresión, la tecnología de lectura y las características físicas del código de barras.
- Sección 5.3 – *Requisitos aplicables a la verificación de los datos biométricos en los documentos de identidad de la gente de mar*, por los que se determina el procedimiento de verificación de la identidad a partir de los datos biométricos almacenados en los DIM.
- Sección 5.4 – *Requisitos aplicables a las bases de datos de los documentos de identidad de la gente de mar*, correspondientes tanto a las bases de datos de los códigos de barras como a las bases electrónicas de datos nacionales de los DIM.

En el anexo A (en inglés) se facilita una descripción pormenorizada del formato del código de barras del DIM para huellas dactilares creadas a partir de patrones. En el anexo B se detalla el formato de almacenamiento de las huellas dactilares creadas a partir de patrones en el código de barras de los DIM. En el anexo C se reproduce el documento ISO/IEC WD 19794-3 – formatos de intercambio de datos biométricos – parte 3: datos correspondientes a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003). Finalmente, en el anexo D se reproduce el documento ISO/IEC WD 19794-4 – formatos de intercambio de datos biométricos – parte 4: formato de intercambio basado en una imagen dactilar (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003).

En vista de que este formato de almacenamiento de huellas dactilares se elaboró de conformidad con una serie de proyectos normativos de la ISO, en el supuesto de que la evolución de alguno de dichos proyectos generase alguna incoherencia respecto a los DIM, *tendrá primacía la aplicación del presente documento*.

Se excluyen del ámbito de aplicación del presente informe técnico las cuestiones siguientes:

1) El funcionamiento general de los sistemas de identificación de la gente de mar que incluyen tecnologías biométricas.

2) Los criterios de validación de la identidad de cada marino o de su titulación profesional.

3) Los criterios de expedición de los DIM.

4) La idoneidad de tecnologías distintas de las tecnologías biométricas basadas en patrones dactilares para el programa de los DIM.

5) Los criterios aplicables a las «demás características relativas a la seguridad» mencionadas en la introducción al anexo I del Convenio núm. 185.

6) Las cuestiones medioambientales que revisten importancia en el entorno marítimo, como la corrosión cristalina y salina, que no guardan relación con lo que es el perfil biométrico, por lo que deberían abordarse en la sección referente a las condiciones de adquisición de los DIM.

7) Valoración del riesgo en la aplicación.

2. Cumplimiento

Se considerará que los sistemas biométricos se ajustan a la presente normativa cuando cumplan correctamente todas las funciones obligatorias definidas en la sección 5, relativa a los *Requisitos biométricos aplicables a los documentos de identidad de la gente de mar*, en el anexo A, titulado *SID Pattern-Based Fingerprint Barcode Format* (formato del código de barras de los documentos de identidad de la gente de mar para huellas dactilares formadas a partir de patrones), y en el anexo B, titulado *SID Barcode Pattern-Based Fingerprint Storage Format (formato del código de barras, para el almacenamiento en los documentos de identidad de la gente de mar, de huellas dactilares formadas a partir de patrones)*.

Cuando se preparó la presente publicación, los requisitos fijados por la OIT y la madurez de las normas internacionales aplicables a las tecnologías biométricas referentes a las huellas dactilares no permitían que se adoptase cualquier tecnología ni característica biométrica para elaborar los DIM. En la presente normativa se fijan los requisitos que habrán de permitir la interoperabilidad internacional de los componentes biométricos de las huellas dactilares creadas a partir de patrones que se almacenarán en la próxima generación de DIM.

3. Referencias

Este perfil biométrico se está elaborando antes de haberse completado los proyectos de normas atinentes a él. Los proyectos de normas mencionados en esta sección llevarán el número de registro del documento SC37 (número «N») y la fecha de publicación del proyecto indicado. En anexo al presente documento se facilitará una copia de todos los proyectos de ***normas imperativas*** (véase sección 3.1). En vista de que el formato de almacenamiento de las huellas dactilares se elaboró conforme a proyectos normativos de la ISO, en el supuesto de que la evolución de dichos proyectos originase alguna incoherencia respecto a los DIM, *tendrá primacía la aplicación del presente documento*.

3.1. Normas imperativas

a) ISO/IEC FCD 19784 — tecnologías de la información — interfaz de programación de aplicaciones para identificación biométrica (BioAPI) (ISO/IEC JTC 1 SC37 N núm. 55, de 17 de diciembre de 2002). (También se trata de una norma ANSI/INCITS: ANSI/INCITS 358-2002 — tecnologías de la información — especificación BioAPI.)

b) ANSI/INST-ITL 1-2000 — formato de datos para el intercambio de información sobre huellas dactilares — cuadro 5.

c) ISO/IEC FDIS 15415 — tecnologías de la información — técnicas de identificación automática y de captura de datos — Especificación de prueba de calidad de impresión de los símbolos de los códigos de barras — símbolos bidimensionales.

d) ISO/IEC 15438:2001 — tecnologías de la información — técnicas de identificación automática y de captura de datos — especificaciones para los símbolos de los códigos de barras — PDF417.

e) ISO/IEC WD 19794-3 — formatos de intercambio de datos biométricos — parte 3: datos correspondientes a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003). (Se trata también de una norma ANSI/INCITS: ANSI/INCITS 377 — formato de intercambio basado en patrones dactilares.)

f) ISO/IEC WD 19794-4 — formatos de intercambio de datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003).

g) ISO/IEC 8859-15:1999 — tecnologías de la información — series de caracteres gráficos codificados en un solo octeto — parte 15: alfabeto latino núm. 9.

h) ISO 3166-1:1997 – códigos para la representación de nombres de países y sus demarcaciones administrativas – parte 1: códigos nacionales.

i) ISO/IEC 9945-1:2003 — tecnologías de la información — interfaz portátil de sistemas operativos (POSIX) — parte 1: definiciones básicas.

3.2. Documentos de referencia

j) Documento 9303 de la OACI — documentos de viaje de lectura mecánica (parte 1, 5.ª edición, 2003; parte 3, 2.ª edición, 2002).

k) Documento ANSI/NIST-ITL-1-2000, formato de datos normalizado para el intercambio de información correspondiente a huellas dactilares, características faciales, cicatrices y tatuajes (SMT).

l) Documento ISO/IEC 7810:2003 — tarjetas de identificación — características físicas.

3.3. Normativa y documentación adicionales que deberían elaborarse o a las que debería darse prioridad para su utilización por la gente de mar

m) Norma aplicable al perfil de aplicación para los DIM.

n) Norma aplicable a la comprobación e información en materia de eficacia e interoperabilidad de los DIM.

o) Un documento de orientación adecuado y fácil de utilizar a la hora de tomar las huellas dactilares a fin de facilitar al personal encargado la tarea de registro y verificación con miras a la obtención de resultados coherentes y fiables.

4. Definiciones

Los autores han procurado velar por que los conceptos, las definiciones, los símbolos y las abreviaturas utilizados en el presente informe técnico se ajusten a la nueva norma de armonización

de la terminología relativa a la biometría que está elaborando el Grupo de Trabajo 1 de la ISO/IEC JTC 1 SC37. A continuación se facilita al lector una definición de los conceptos importantes.

4.1. Conceptos y definiciones

4.1.1. Perfil de aplicación

Series o combinaciones constitutivas de normas básicas destinadas a la realización de funciones específicas. Los perfiles de aplicación permiten determinar la utilización de opciones específicas en las normas básicas, amén de establecer una conexión entre las aplicaciones y garantizar la interoperabilidad de los sistemas.

4.1.2. Biométrico

Adjetivo. Relativo a la biometría.

NB: no debería utilizarse el vocablo «biométrico» como sustantivo.

4.1.3. Autentificación biométrica/autentificar por medios biométricos

Utilización de la verificación o la identificación biométrica para validar la autenticidad de los datos correspondientes a una persona.

4.1.4. Bloque de datos biométricos (BDB)

Bloque de datos con formato definido que contiene una o más muestras o plantillas biométricas.

4.1.5. Identificación biométrica/identificar por medios biométricos

Asociación de una muestra biométrica a una entrada en una base de datos biométricos, contrastando la muestra biométrica con todas las muestras biométricas almacenadas en la base de datos, y generando índices de semejanza entre las muestras así comparadas.

4.1.6. Registro de identificación biométrica (BIR)

Estructura de datos que contiene un BDB, además de información para determinar el formato de éste y, eventualmente, indicaciones adicionales acerca de si, por ejemplo, el BDB lleva firma o codificación digital.

4.1.7. Registro de datos biométricos con fines de intercambio (BIDR)

Estructura de datos correspondientes a una persona, que contiene un BIR (véase 4.1.6) e información específica sobre los sistemas, aplicaciones y funciones de identificación de la gente de mar.

4.1.8. Muestra biométrica

Información obtenida a partir de un dispositivo biométrico, ya sea directamente o mediante un proceso determinado.

4.1.9. Verificación biométrica/verificar por medios biométricos

Confirmar que una muestra biométrica coincide con la muestra biométrica procesada, almacenada y asociada a la identidad declarada de la persona interesada, mediante un cotejo de plantillas, la generación de índices y la comparación de estos índices con el umbral de semejanza.

4.1.10. Registrar mediante procedimientos biométricos

Acopio de una o más muestras biométricas de una persona y ulterior preparación y almacenamiento de una o más muestras biométricas procesadas y de datos asociados que sean representativos de la identidad de la persona.

4.1.11. Código nacional

Código nacional numérico de tres dígitos determinado en la norma ISO 3166-1.

4.1.12. Integridad de los datos

Propiedad inherente al sistema respecto a los datos materialmente almacenados, por ejemplo, en los DIM o en las bases electrónicas de datos nacionales de DIM, de forma que resulte imposible alterar la información sin dejar rastros.

4.1.13. Confidencialidad de los datos

Propiedad inherente al sistema respecto a los datos materialmente almacenados, por ejemplo, en los DIM o en las bases electrónicas de datos nacionales de DIM, de forma que no puedan acceder a dichos datos ni modificarlos más que las personas debidamente autorizadas, siempre que se trate de aplicaciones accesibles a estos efectos y que se disponga del potencial tecnológico para ello.

4.1.14. Interoperabilidad mundial de los datos biométricos almacenados en los DIM

Aceptación mundial de los bloques de datos biométricos correspondientes a huellas dactilares almacenados en un código de barras bidimensional impreso en el DIM con miras a la verificación de la identidad del marino.

4.1.15. Terminado en cero

Terminado en un octeto cero (0x00).

4.1.16. Tiempo real

Vinculado o relativo a un modo de operación informática en que el ordenador recaba datos, los tiene en cuenta y utiliza los resultados correspondientes para controlar los procesos mientras se producen.

4.1.17. Segundos desde la época (SSE)

Segundos desde la época (en un entero sin signo de 32 bits) del día especificado según lo dispuesto en la norma ISO/IEC 9945-1:2003, sección 4.14. Si bien se aceptan todos los segundos de cada día, cuando se desconozca el segundo exacto del día de que se trate, la aplicación realizada con el DIM se retrotraerá supletoriamente al primer segundo del mismo día.

4.1.18. Empleo del futuro

Según la práctica legislativa, el empleo del futuro designa prácticas imperativas.

4.1.19. Empleo del condicional

Según la práctica legislativa, el empleo del condicional designa prácticas recomendadas, que por ende no son obligatorias.

4.1.20. Tren textual

Tren de datos inscritos en caracteres del alfabeto latino según la norma ISO 8859-15:1999.

5. Requisitos biométricos aplicables a los documentos de identidad de la gente de mar

5.1. Requisitos biométricos aplicables a los documentos de identidad de la gente de mar creados a partir de patrones dactilares

Se imprimirán, en forma de números en un código de barras ajustado a la norma indicada en el presente documento, dos plantillas biométricas creadas a partir de patrones dactilares correspondientes al marino al que se haya expedido el documento. En el Convenio núm. 185 de la OIT se han fijado las condiciones que debe reunir el sistema resultante, las cuales se destacan a continuación. Las autoras de este perfil biométrico se han basado en la estrategia de cumplimiento.

- La huella dactilar podrá «obtenerse sin que ello implique injerencia en la privacidad del titular, molestia, riesgo para su salud, o lesión de su dignidad;» (Convenio Internacional del Trabajo núm. 185, artículo 3, apartado *a)* del párrafo 8).

  Con este requisito, se pretende evitar que los marinos perciban la adquisición y la verificación de sus huellas dactilares como una injerencia en la privacidad y una lesión de la dignidad. Del mismo modo, los sistemas biométricos y los lectores de códigos de barras se instalarán atendiendo a criterios ergonómicos, para no incomodar a los marinos. Tanto durante la utilización de este sistema como una vez terminada ésta, se prevendrá todo riesgo para la salud. Estos sistemas se desinfectarán automáticamente al cabo de cada utilización, a fin de evitar la propagación de gérmenes que pudieran derivarse del contacto con los componentes del sistema, y a fin de que utilizar el dispositivo de adquisición de huellas dactilares no resulte más arriesgado que, por ejemplo, tocar el pomo de una puerta.

- «Los datos biométricos [serán] visibles en el documento y no [podrán] reconstituirse a partir de la plantilla o de otras representaciones;» (Convenio Internacional del Trabajo núm. 185, artículo 3, apartado *b)* del párrafo 8).

  Con este requisito se pretende dificultar suficientemente la reconstitución de huellas dactilares reales (entiéndase «imágenes de huellas dactilares»), o la elaboración de dispositivos fraudulentos que puedan servir para dar una representación desviada de la intención o la presencia de un marino, a partir de los datos biométricos almacenados en el código de barras. También es necesario que los datos biométricos se consideren visibles una vez impreso el código de barras con los datos biométricos correspondientes a la huella dactilar en los DIM de próxima generación, y que la decisión de la OIT de utilizar plantillas creadas a partir de patrones dactilares permita evitar una utilización abusiva de los datos biométricos almacenados y, por consiguiente, la utilización de la identidad de los marinos con fines abusivos.

- «El material necesario para proveer y verificar [la muestra biométrica es] fácil de utilizar y, en general, asequible para los gobiernos a bajo costo;» (Convenio Internacional del Trabajo núm. 185, artículo 3, apartado *c)* del párrafo 8).

  Resulta claro que el requisito de fácil utilización podrán cumplirlo y, de hecho, lo cumplirán los operadores y los usuarios del sistema mediante la utilización de un sistema biométrico ergonómico. También resulta claro que la opción seleccionada por la OIT para almacenar en un código de barras datos biométricos formados a partir de patrones dactilares atiende al requisito de «asequibilidad general para los gobiernos a bajo costo», pues esta alternativa requiere el empleo de aparatos de baja resolución y de dispositivos de captura de huellas dactilares menos onerosos.

- «El material [utilizado] para verificar [la muestra biométrica puede] utilizarse con comodidad y fiabilidad en los puertos y en otros lugares, incluso a bordo de los buques, donde las autoridades competentes suelen proceder a las verificaciones de identidad;» (Convenio Internacional del Trabajo núm. 185, artículo 3, apartado *d)* del párrafo 8).

  Con este requisito se pretende que los sistemas biométricos y de lectura de tarjetas puedan utilizarse de manera fiable a bordo de los buques, en los puertos y en otros lugares, de forma que los sistemas no presenten un grado sensibilidad inhabitual a la salinidad corrosiva de la atmósfera, característica de dichos lugares.

- «El sistema en que se haya de [proceder a una autentificación biométrica] (con inclusión del material, las tecnologías y los procedimientos de utilización) [permitirá] obtener unos resultados uniformes y fiables en materia de autentificación de la identidad.» (Convenio Internacional del Trabajo núm. 185, artículo 3, apartado *e)* del párrafo 8).

  La «uniformidad» presupone el cumplimiento de lo previsto en el presente informe técnico en aras de la interoperabilidad. También presupone que los sistemas biométricos comerciales han de ser fiables a efectos de «autentificar la identidad» (entiéndase «verificar la identidad») para los marinos que utilicen estos sistemas.

5.1.1. Procedimiento de registro de los datos biométricos

El presente informe técnico no versa sobre la totalidad del procedimiento instaurado por la OIT para la comprobación de identidad a partir de los DIM, sino que se centra en aquella parte del procedimiento referente al registro de los datos biométricos. Todo agente habilitado para expedir DIM deberá introducir en el sistema de registro los datos personales enumerados en el anexo A. Debería tomarse una huella del dedo índice de cada mano [2]. De faltar la yema del dedo índice o de haber sido ésta dañada hasta el punto de que no pueda producirse una huella dactilar fiable o de que ésta no se pueda registrar dada su escasa calidad, se tomará la huella de otro dedo, que puede ser un pulgar, para garantizar coherencia y eficacia operativa, y maximizar la comodidad del marino. El orden de presentación de los dedos para su registro será normalmente el siguiente:

- dedo índice de la mano derecha;
- dedo índice de la mano izquierda;
- dedo pulgar de la mano derecha;
- dedo pulgar de la mano izquierda;
- dedo corazón de la mano derecha;
- dedo corazón de la mano izquierda;
- dedo anular de la mano derecha;
- dedo anular de la mano izquierda;
- dedo meñique de la mano derecha, y
- dedo meñique de la mano izquierda.

El agente encargado de expedir los DIM especificará qué dedos se tomaron para el registro biométrico y la información quedará inscrita en el encabezamiento de la plantilla biométrica para su almacenamiento en el código de barras del DIM (véase anexo B).

En el sistema debería preverse automáticamente un índice de calidad, o bien convendría que el personal encargado del registro dispusiera de un indicador, de calidad mínima aceptable para garantizar que se generen plantillas de buena calidad (recabadas o adquiridas). Deberían registrarse solamente las huellas dactilares de máxima calidad y deberían almacenarse las plantillas de estas huellas de forma que se logren resultados de comprobación fiables. El marino deberá poder

[2] Se toman las huellas dactilares de dos dedos para incrementar la fiabilidad y la eficacia del sistema. Se ha elegido el dedo índice para las huellas dactilares principales porque en la mayoría de los casos es el más fácil de colocar en el dispositivo de adquisición de huellas dactilares, para la mayor comodidad del marino (artículo 3, párrafo 8, requisito 1).

cerciorarse de que sus datos biométricos de referencia, que se almacenarán en su DIM, puedan utilizarse para facilitar la verificación biométrica, especialmente en el lugar de expedición.

El sistema de reconocimiento biométrico de las huellas dactilares deberá:

- Presentar en la pantalla indicaciones para el agente encargado de expedir los DIM y para el marino a fin de facilitar el registro. Estas indicaciones versarán sobre el procedimiento, la valoración de la calidad y la colocación adecuada de los dedos.
- Utilizar mediciones de contenido y calidad a fin de garantizar la calidad de adquisición de las plantillas, y ofrecer la posibilidad de contrastar las medidas de contenido y calidad con los valores mínimos prefijados a fin de determinar si procede indicar al marino que vuelva a presentar el mismo dedo o el dedo siguiente para un nuevo registro.
- Efectuar una medición a fin de indicar la calidad de la plantilla de la huella dactilar adquirida y facilitar información visual al operador (agente encargado de la expedición del DIM) y a la persona que se registre (el marino) acerca de la imagen de la huella dactilar tomada.
- En el caso de que el sistema biométrico no logre adquirir una plantilla aceptable para un dedo determinado, permitir al agente encargado de la expedición del DIM proceder al registro de otro dedo.
- Permitir al marino proceder a una comprobación biométrica antes de que se imprima el código de barras de su DIM, a fin de que la plantilla adquirida corresponda a la huella dactilar registrada y sea aceptable desde un punto de vista operativo para el marino. Se indicará que los datos corresponden (identidad comprobada) cuando el índice de semejanza supere los valores mínimos fijados para la verificación (véase 5.3.1), y se indicará que no corresponden (identidad no comprobada) cuando el índice de semejanza no supere los valores mínimos para el reconocimiento.
- Indicar el número de dedos que se haya conseguido registrar.
- Permitir al agente encargado de expedir los DIM examinar los datos textuales introducidos, modificarlos según se le haya indicado, e imprimir el código de barras del DIM.
- Corroborar el reconocimiento biométrico del marino mediante el DIM impreso con arreglo a lo indicado en la sección 5.3.1.

5.1.2. Documentación para el registro de los datos biométricos

Se facilitará al personal una documentación fácil de utilizar sobre la manera de proceder al registro a fin de que se registren huellas dactilares de buena calidad y se almacenen en el DIM plantillas de huellas dactilares que sean igualmente de buena calidad.

5.1.3. Adquisición de las huellas dactilares

Tanto durante la fase de registro como durante la de verificación, el dispositivo de adquisición de huellas dactilares tomará plantillas biométricas a partir de patrones dactilares con arreglo a lo previsto en el cuadro 1 del anexo A del proyecto de norma ISO/IEC WD 19794-4 — formatos de intercambio de datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003) [3] (véase anexo D al presente documento para consultar la versión integral del proyecto de norma) con un nivel mínimo de calidad de adquisición de datos de huellas dactilares de grado 3 [4], según se especifica *infra*:

[3] El Grupo de Trabajo 3 de la ISO/IEC JTC 1 SC37 está revisando este proyecto de normativa. Esperamos que los parámetros de calidad de grado 3 se mantengan cuando la norma sea adoptada. Con todo, para los DIM primarán los parámetros indicados en el presente documento.

[4] El nivel de calidad 3 para la adquisición de los datos correspondientes a las huellas dactilares es aceptable para las imágenes que hayan de utilizarse para generar plantillas de huellas dactilares basadas a partir de patrones. Obsérvese que la calidad de la adquisición de los datos

- resolución de exploración: 98 píxeles/cm (250 píxeles/pulgada);
- profundidad de píxel: 3 bits;
- gama dinámica (escala de grises): 8;
- certificación: ninguna.

El dispositivo de adquisición de las huellas dactilares producirá una imagen de 12,7 mm por 12,7 mm (0,5 pulgadas por 0,5 pulgadas) de la huella dactilar, y la imagen se centrará preferiblemente en el centro de la huella dactilar.

Cuando se transmita la imagen de la huella dactilar al algoritmo de extracción de la plantilla, por ejemplo desde el dispositivo de adquisición hasta el ordenador, los datos saldrán sin comprimir o serán comprimidos sin pérdida.

5.1.4. Plantillas de las huellas dactilares

El algoritmo extraerá una plantilla a partir de la imagen de la huella dactilar adquirida con arreglo a la norma ISO/IEC WD 19794-3 — formatos de intercambio de datos biométricos — parte 3: datos correspondientes a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003). Las plantillas de huellas dactilares se almacenarán en la base electrónica de datos nacional (base de datos mencionada en el Convenio) y en el código de barras bidimensional PDF417 del DIM durante el registro, y se utilizará para proceder a las comparaciones durante la verificación.

Las plantillas tomadas de patrones dactilares han de almacenarse con arreglo a las siguientes consideraciones:

1. Deben almacenarse dos plantillas de huellas dactilares del marino en el código de barras PDF417 del DIM.

   a) La memoria necesaria para almacenar la *imagen* de las huellas de dos dedos, ya esté codificada o no lo esté, será superior a la capacidad de almacenamiento del código de barras bidimensional PDF417 del DIM.

   b) El tamaño de las plantillas basadas en *minucias* dactilares varía en función del número de minucias detectadas en cada dedo [5]. Según una solicitud de información cursada por la OIT en diciembre de 2003 a los vendedores de productos biométricos, las plantillas de minucias contienen por regla general de 5 a 60 minucias. Con todo, el número máximo de minucias que puede almacenarse en la memoria del código de barras PDF417 del DIM es de 96 minucias, o sea, de 48 minucias por dedo. Así pues, para que en el código de barras del DIM quepan plantillas basadas en minucias para dos dedos, deben limitarse el número de minucias admitido y el tamaño total del registro. Se examinaron dos posibilidades para limitar el tamaño de las plantillas tomadas a partir de minucias. La primera consistiría en fijar un número máximo de minucias almacenables por huella dactilar y designar el método previsto por la OIT para los DIM a fin de ordenar las minucias jerárquicamente con miras a su inclusión en la plantilla. La segunda posibilidad consistiría en indicar tan sólo el número máximo de minucias almacenables en el código de barras PDF417 del DIM previsto por la OIT. No se consideró viable ninguna de estas dos posibilidades por las siguientes razones:

      i) De las respuestas de los vendedores de productos biométricos a la solicitud de información cursada por la OIT en diciembre de 2003 se desprende que no existe un método uniforme para truncar las plantillas. El hecho de ajustarse a un método de truncamiento específico puede tener consecuencias impredecibles en los resultados de cada sistema biométrico, que no pueden garantizarse mientras no se hayan realizado las pruebas exhaustivas necesarias en un laboratorio debidamente certificado para ello.

correspondientes a las huellas dactilares es distinta e independiente de la calidad de la imagen de impresión del código de barras del DIM.

[5] Norma ISO/IEC WD 19794-2 — formatos de intercambio de datos biométricos — parte 2: datos correspondiente a minucias dactilares (ISO/IEC JTC 1 SC37 N 340, de 7 de octubre de 2003).

ii) Además, si un vendedor trunca sus plantillas[6] para ajustarse a los límites dimensionales señalados por la OIT para el código de barras PDF417 del DIM, no podrán predecirse ni garantizarse las consecuencias en el funcionamiento de ningún sistema de reconocimiento biométrico, sea cual fuere su vendedor, sin haberse procedido primero a pruebas exhaustivas en un laboratorio certificado a estos efectos.

iii) Se garantiza que antes de adoptarse esta estrategia se procederá a una prueba para valorar las consecuencias que tendrá el hecho de imponer una dimensión máxima para las plantillas y para valorar las consecuencias que tendría adoptar un método específico de ordenación jerárquica de las minucias para su inclusión o su truncamiento.

c) Las plantillas basadas en *patrones* dactilares tienen un tamaño fijo y pueden almacenarse dos patrones dactilares dentro de los límites de la memoria del código de barras PDF417 del DIM conforme a la norma ISO/IEC WD 19794-3 — formatos de intercambio de datos biométricos — parte 3: datos correspondientes a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003). (Se ha conferido a este documento rango de norma, que se titula ANSI/INCITS 377 — formato de intercambio basado en patrones dactilares.) Se ha sometido oficialmente a prueba esta estrategia de plantillas de dimensiones fijas creadas a partir de patrones.

2. Los sistemas autorizados serán generalmente asequibles para los gobiernos al costo más bajo posible sin merma de su fiabilidad, en cumplimiento del objetivo señalado en el Convenio núm. 185.

a) Con arreglo a la norma ISO/IEC WD 19794-4 — formatos de intercambio de datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003), la resolución de imagen necesaria para los algoritmos basados en *patrones* es inferior a la necesaria para los algoritmos basados en *minucias* (250 píxeles por pulgada frente a 500 píxeles por pulgada). Con los algoritmos basados en *patrones* pueden utilizarse dispositivos de adquisición de huellas dactilares de 250 píxeles por pulgada, menos onerosos.

3. En virtud del Convenio núm. 185, resultará imposible reconstituir los datos biométricos a partir de la plantilla o de otras representaciones.

a) Los datos biométricos almacenados en el DIM no deberían permitir una utilización abusiva de las plantillas biométricas de los marinos. Más en particular, deberá ser suficientemente difícil que a partir de los datos biométricos almacenados en el código de barras pueda reconstituirse una huella dactilar (entiéndase una «imagen de huella dactilar»), o puedan elaborarse dispositivos fraudulentos que permitan dar información falsa sobre una huella dactilar de un marino.

b) Podría resultar posible reconstituir la imagen de una huella dactilar o elaborar un dispositivo fraudulento que permita producir datos falsos sobre la huella dactilar de un marino mediante la información almacenada en plantillas de huellas dactilares basadas en *minucias* o en *imágenes*[7]. No se sabe de ningún método que permita utilizar datos almacenados en plantillas de huellas dactilares basadas en *patrones* para reconstituir la

[6] Aunque en fechas recientes se ha sometido a examen de la ISO una propuesta de normalización del truncamiento de plantillas basadas en minucias, no es seguro que estén disponibles los productos necesarios para aplicar dicho método y dado el plazo fijado por la OIT no queda tiempo para someter esta tecnología a prueba antes de que se publique el presente perfil biométrico.

[7] Bromba, M.: «On the reconstruction of biometric raw data from template data», 9 de julio de 2003. Cargar de la página web: http://www.bromba.com/knowhow/temppriv.htm.

imagen de una huella dactilar o elaborar un dispositivo fraudulento que permita producir información sobre la huella dactilar de un marino [8].

Con arreglo a lo indicado en las normas ISO/IEC WD 19794-3 — formatos de intercambio de datos biométricos — parte 3: datos correspondientes a patrones dactilares (ISO/IEC JTC 1 SC37 N 313, de 3 de octubre de 2003), las características de la plantilla biométrica creada a partir de patrones dactilares para los DIM previstos por la OIT se detallan en los anexos A, B y C. La estructura de los datos del código de barras del DIM se resume a continuación:

- encabezamiento BioAPI — 16 octetos;
- encabezamiento para los datos correspondientes a patrones de huellas dactilares — 32 octetos;
- dos plantillas tomadas de patrón dactilar — 520 octetos;
- cada plantilla de patrón dactilar constará de 224 células: 14 células por fila, x 16 filas. Cada célula tendrá una profundidad angular de 3 bits, una profundidad de longitud de onda de 3 bits, y una profundidad de desplazamiento de fase de 3 bits;
- la representación digital de los datos se describe en el anexo A — 120 octetos;
- tamaño total del código de barras del DIM — 688 octetos.

5.2. Requisitos aplicables al código de barras de los documentos de identidad de la gente de mar y a los lectores de estos códigos

5.2.1. Formato del código de barras

El formato del código de barras del DIM se ajustará a lo dispuesto en el anexo A. El código de barras de los DIM para huellas dactilares creadas a partir de patrones, contendrá 688 octetos de datos y 64 símbolos de datos para un nivel de corrección de errores de 5. El código de barras contendrá la información de la plantilla biométrica, así como una información que se imprimirá sobre el DIM, a saber: la autoridad expedidora; el número de identidad personal facultativo; el nombre completo del marino; el número de documento único; la fecha de caducidad del documento; la nacionalidad del marino; la fecha y el lugar de nacimiento del marino, su sexo y el lugar y la fecha de expedición del DIM (véase anexo A). Las plantillas biométricas correspondientes al marino, que admitirán dos huellas dactilares, se formatearán con arreglo a lo indicado en el anexo B, en que se define el bloque de datos biométricos de 568 octetos indicado en el anexo A. Este bloque de datos biométricos de 568 octetos, sumado a la información del encabezamiento de 120 octetos descrito en el anexo A, configura el código de barras del DIM, que tiene una capacidad de 688 octetos.

Se aplicará la tecnología del código de barras bidimensional PDF417 atendiendo a las consideraciones siguientes:

- que los símbolos PDF417 se ajusten a los requisitos de capacidad de almacenamiento de datos de esta aplicación;
- que los símbolos PDF417 puedan leerse con un escáner de lectura bidimensional o con escáneres normales CCD (con dispositivo de transferencia de carga) o láser y un programa informático especial de descodificación. En cambio, los escáneres de lápiz de contacto no leerán los símbolos. Esta amplia gama de productos tecnológicos lectores de código de barras, asequibles y a la venta en el mercado, facilitará la verificación biométrica de la identidad de los marinos.

El tamaño y la ubicación del código de barras se ajustarán a las características preceptuadas por la Organización de Aviación Civil Internacional (OACI), en la parte 1 del documento 9303 (5.ª edición, 2003) y en la parte 3 del documento 9303 (2.ª edición, 2002), y según se reseña más adelante:

[8] Hill, C.J.: «Risk of Masquerade Arising from the Storage of Biometrics», B.S. Thesis, Universidad Nacional de Australia, 2001. Cargar de la página web: http://chris.fornax.net/biometrics.html.

- para los DIM con formato de libreta, el tamaño máximo del código de barras será de 21,5 mmx86 mm, incluidas las zonas de silencio, según se especifica en la parte 1 del documento 9303 de la OACI — pasaportes de lectura mecánica — IV especificaciones técnicas — sólo para los pasaportes de lectura mecánica — anexo E (normativo) empleo de códigos de barras opcionales, facultativos, en la página de datos del pasaporte de lectura mecánica;
- para los DIM con formato de tarjeta, el tamaño máximo del código de barras será de 27,8 mmx85,6 mm [9], inclusive las zonas de silencio (véase parte 3 del documento 9303 de la OACI — documentos de viaje de lectura mecánica oficiales de tamaño 1 y de tamaño 2 — anexo E (normativa) a la sección 4 — empleo del código de barras opcional en el DV-1).

Además, el código de barras del DIM se ajustará a los siguientes requisitos:

- tamaño X: la anchura mínima del módulo de símbolos será de 0,10 mm (de ser posible mayor, para rellenar la zona correspondiente de la tarjeta, hasta un tamaño máximo de 0,175 mm;
- tamaño Y: la altura mínima de la fila será de 0,511 mm (el triple de la dimensión X, de ser posible, mayor, para rellenar la zona correspondiente de la tarjeta, hasta un tamaño máximo de 0,525 mm);
- nivel 5 de corrección de errores, según se recomienda en la norma ISO/IEC 15438:2001, anexo E, y en la parte 3 del documento 9303 de la OACI (2.ª edición, 2002);
- número de columnas de símbolos informativos = 16 [10];
- número de filas necesario para incluir los datos (40 filas [11]).

5.2.2. Tecnología empleada en las impresoras y especificaciones de impresión

El código de barras PDF417 para DIM se imprimirá con arreglo a la norma ISO/IEC 15438:2001. Los símbolos del código de barras bidimensional PDF417 pueden imprimirse con las mejores marcas de impresoras profesionales térmicas, láser y chorro de tinta. La próxima generación de impresión de códigos de barras de gran calidad se ajustará al proyecto de norma ISO/IEC FDIS15415 — especificación de prueba de calidad de impresión de los símbolos de los códigos de barras — símbolos bidimensionales, con la signatura 3.0/05/660. Esta signatura corresponde a la categoría genérica de 3,0 atribuida a los símbolos, resultado de una apertura de 0,125 mm y una longitud de onda de 660 nm.

[9] Ello significa que la próxima generación de DIM con formato de tarjeta será de tamaño 1 y no 2 correspondiente a los documentos de viaje de lectura mecánica, según se especifica en la parte 3 del documento 9303 de la OACI (2.ª edición, 2002).

[10] El Sr. Sprague Ackley, experto de renombre internacional en tecnologías para códigos de barras bidimensionales PDF417, declara que, «si bien no se sabe todavía a ciencia cierta a partir de cuándo los reproductores de imágenes bidimensionales empiezan a tener dificultades con los símbolos PDF417 con varias columnas, es casi seguro que la inclusión de 25 columnas de datos frustrarán el funcionamiento de los reproductores de imágenes bidimensionales». La utilización de 16 columnas de datos (20 en total) permitirá emplear una tecnología de lectura de códigos de barras de exploración bidimensional con suficiente espacio vertical para incluir en el DIM el código de barras y los datos.

[11] La derivación del número de filas del formato del código de barras del DIM correspondiente a patrones se detalla a continuación: se prevén 688 octetos de datos en cada DIM. Cada palabra de código puede almacenar 1,2 octetos. Por tanto, hay 688/1,2 = 574 palabras de código. Se necesitan 64 palabras de código adicionales para los códigos de corrección de errores de nivel 5, además de una palabra de código para toda la extensión del código de barras. Por tanto, hay un total de 574 + 64 + 1 = 639 símbolos informativos en el código de barras de los DIM. Hay 16 columnas de datos. Por tanto, se necesitan 639/16 = 40 filas para almacenar los datos en el código de barras de los DIM.

Los códigos de barras de los DIM se imprimirán de forma que el documento tenga la resistencia al desgaste exigible para todo DIM.

La ubicación de la zona de impresión del código de barras se ajustará a las especificaciones de la OACI previstas en la parte 1 del documento 9303 (5.ª edición, 2003) y en la parte 3 del documento 9303 (2.ª edición, 2002).

5.2.3. Tecnología de lectura

Los símbolos de los códigos de barras PDF417 para DIM de próxima generación se leerán con un escáner bidimensional, o con escáneres clásicos CCD o láser, y con un software especial de descodificación que leerá los códigos de barras impresos con arreglo a las secciones 5.2.1 y 5.2.2. En cambio, los escáneres de lápiz de contacto no leerán los símbolos PDF417.

5.2.4. Características físicas del código de barras

La «plantilla biométrica correspondiente a la huella dactilar impresa en forma de números en un código de barras» (Convenio internacional del trabajo núm. 185, anexo I, párrafo 3, *k)*) «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» (Convenio internacional del trabajo núm. 185, anexo I. Esta protección mejorará también la resistencia del código de barras al tiempo.

«Los datos biométricos [serán] visibles en el documento» (Convenio internacional del trabajo núm. 185, artículo 3, apartado *b)* del párrafo 8). Este requisito debe interpretarse en el sentido de que los datos biométricos se considerarán visibles cuando el código de barras en que estén almacenados los datos biométricos correspondientes a las huellas dactilares se imprima en el DIM de próxima generación. El código de barras será visible cuando esté impreso en el DIM. Además, el marino podrá ver una representación binaria de la plantilla integrada en el código de barras y verificar personalmente los datos biométricos utilizando el DIM como fuente de referencia en los puestos de expedición de dichos documentos.

5.3. Requisitos aplicables a la verificación de los datos biométricos en los documentos de identidad de la gente de mar

5.3.1. Procedimiento de verificación de los datos biométricos

Se explorará el código de barras del DIM con un lector especial, que leerá la información del encabezamiento y de la plantilla correspondientes. En el encabezamiento constará qué huellas dactilares están almacenadas en el código de barras.

El sistema invitará al marino a que coloque el primer dedo para la lectura de la plantilla dactilar almacenada en el código de barras.

Si el dedo correspondiente al primer dedo registrado está ocupado, está dañado o no fue captado, o si el resultado del reconocimiento no supera el valor umbral de semejanza al cabo de tres intentos, el sistema pedirá al marino que coloque el segundo dedo inscrito en el dispositivo de adquisición biométrica. Si las características del dedo explorado coinciden con las plantillas correspondientes almacenadas en el código de barras, se comprobará la identidad coincidente del marino. Si ninguno de los dedos que se exploren se ajustan a las plantillas correspondientes almacenadas en el código de barras, el sistema indicará que no ha conseguido comprobar la información. Si, al cabo del tercer intento, con los dos dedos inscritos el sistema indica que no ha conseguido verificar la información, no se permitirán más intentos con el mismo DIM sin que intervenga un miembro del personal autorizado para proceder a la comprobación.

El sistema de reconocimiento biométrico para huellas dactilares deberá:

- recuperar la plantilla del código de barras bidimensional PDF417 del DIM;
- pedir a la autoridad que verifique el DIM y al marino que coadyuve, a la verificación, y facilitar indicaciones de procedimiento, información sobre la colocación adecuada de los dedos y los resultados de la verificación;

- indicar al marino que coloque el dedo apropiado en el captor de imagen;
- comparar la imagen de la huella dactilar adquirida con la plantilla correspondiente almacenada en el código de barras;
- facilitar una indicación de reconocimiento (identidad comprobada) si el resultado del reconocimiento supera el umbral de semejanza, y señalar un desajuste (identidad no comprobada) si el resultado del reconocimiento es inferior al umbral de semejanza;
- exigir la intervención del personal de verificación cuando, al cabo de tres intentos con cada dedo, el marino no consiga que se reconozca ninguno de sus dedos registrados.

El sistema biométrico para huellas dactilares debería:

- estar dotado de un umbral de semejanza tal que tanto la tasa de falsas aceptaciones como la de falsos rechazos sean inferiores al 1 por ciento de toda la población;
- dotarse de medidas de contenido y calidad proporcionales a la calidad métrica requerida para el registro;
- ofrecer, con carácter facultativo, una medida que indique la calidad de la plantilla de la huella dactilar adquirida.

5.3.2. Documentación para la verificación de los datos biométricos

Se facilitará al personal una documentación fácil de utilizar sobre la manera de proceder a la verificación.

5.4. Requisitos aplicables a la base de datos de los documentos de identidad de la gente de mar

5.4.1. Base de datos de los códigos de barras

«Los marinos [tendrán] fácil acceso a las máquinas que les [permitirán] examinar los datos que se refieran a ellos y no puedan leerse a simple vista. Dicho acceso deberá ser facilitado por la autoridad expedidora, o en su nombre» (Convenio internacional del trabajo núm. 185, párrafo 9 del artículo 3). «La plantilla biométrica [corresponderá] a una huella dactilar impresa en forma de números en un código de barras, acorde con una norma» [la presente norma] (Convenio internacional del trabajo núm. 185, anexo I).

La autoridad expedidora dará a los marinos acceso a las máquinas que les permitirán consultar los datos almacenados en el código de barras bidimensional PDF417 de su DIM. El marino podrá verificar si las plantillas de las huellas dactilares almacenadas en su tarjeta coinciden con las huellas registradas. Los datos que no sean relativos a las huellas dactilares se presentarán en forma de texto.

5.4.2. Base electrónica de datos nacional de los DIM

En el Convenio núm. 185 de la OIT se prevé una serie de requisitos que cada Miembro debe o debería cumplir en relación con la base electrónica de datos nacional de los DIM. Estos requisitos, que incidirán en la aplicación y la utilización del sistema de reconocimiento biométrico, se destacan a continuación junto con la estrategia de cumplimiento preconizada por las autoras del presente perfil biométrico.

- «Los datos que deberán suministrarse para cada asiento abierto en la base electrónica de datos, que todos los Miembros habrán de mantener al día en virtud de los párrafos 1, 2, 6 y 7 del artículo 4 del presente Convenio [de la Conferencia Internacional del Trabajo] [núm. 185], serán exclusivamente los siguientes:

  1. Autoridad expedidora indicada en el documento de identidad.
  2. Nombre completo del marino, tal como conste en el documento de identidad.

3. Número único del documento.

4. Fecha de caducidad, suspensión o retiro del documento de identidad.

5. Plantilla biométrica que figure en el documento de identidad.

6. Fotografía (de estar almacenada en formato digital).

7. Pormenores sobre toda solicitud de información acerca de los documentos de identidad de la gente de mar.» (Convenio internacional del trabajo núm. 185, anexo II.)

En la base electrónica de datos nacional se registrarán los siete extremos antes enumerados para cada DIM expedido a un marino.

- «A los efectos del presente Convenio, se establecerán restricciones apropiadas a fin de que ningún dato, en particular las fotografías, pueda ser intercambiado, a menos que se instaure un mecanismo que garantice el cumplimiento de las normas aplicables en materia de protección de datos y de privacidad.» (Convenio internacional del trabajo núm. 185, artículo 4, párrafo 6.)

  Se instaurarán mecanismos de control del acceso a la base de datos para proteger la información relativa a los marinos frente a las personas no autorizadas y a toda actuación desviada.

- «Los datos indicados en los puntos del anexo II [al Convenio internacional del trabajo núm. 185] se [introducirán] en la base de datos al tiempo que se expidan los DIM correspondientes.» (Convenio internacional del trabajo núm. 185, anexo III, parte A, párrafo 3, apartado *b)*, inciso i).)

  Las bases electrónicas de datos nacionales de todos los Miembros se actualizarán oportunamente cada vez que se expida un nuevo DIM.

- «Todo Miembro velará por que se conserve en una base electrónica de datos constancia de cada documento de identidad de la gente de mar que haya sido expedido, suspendido o retirado. Deberán adoptarse las medidas necesarias para proteger esta base de datos frente a toda injerencia o acceso no autorizados.» (Convenio internacional del trabajo núm. 185, artículo 4, párrafo 1.) «El documento de identidad de la gente de mar será retirado rápidamente por el Estado que lo haya expedido si se determinase que el marino titular ha dejado de reunir las condiciones requeridas en el presente Convenio.» (Convenio internacional del trabajo núm. 185, artículo 7, párrafo 2.) «La autoridad expedidora debería instaurar procedimientos adecuados para proteger la base de datos, en particular permitir únicamente a los funcionarios especialmente habilitados tener acceso a las entradas de la base de datos o modificar estas últimas, una vez que hayan sido confirmadas por el funcionario responsable de ellas.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 4.2.2.)

  En las bases electrónicas de datos nacionales de los Miembros se incluirá una función de comprobación sobre las operaciones siguientes: la expedición de los DIM, su suspensión y su retiro. Se utilizarán mecanismos para controlar el acceso a la base de datos a fin de proteger la información relativa a los marinos frente a las personas no autorizadas y actuaciones desviadas. Los funcionarios especialmente autorizados de la entidad responsable en cada Estado Miembro deberían tener facultades limitadas para introducir cambios en el diario de comprobación. Los Miembros guardarán constancia de cada uno de estos cambios.

- «[Se adoptarán rápidamente] medidas para actualizar la base de datos cada vez que se suspenda o se retire un DIM.» (Convenio internacional del trabajo núm. 185, anexo III, parte A, párrafo 3, apartado *c).*)

  Las bases electrónicas de datos nacionales de cada Miembro se actualizarán oportunamente cada vez que se suspenda un DIM o que se retire.

- «[Se instaurará] un sistema de prórroga o de renovación para atender a las situaciones en que el marino necesite que se prorrogue o se renueve su DIM, o en que se le haya perdido el DIM.» (Convenio internacional del trabajo núm. 185, anexo III, parte A, párrafo 3, apartado *d).*) «Mientras el solicitante sea titular de un DIM, no se le debería expedir otro DIM.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 3.9.)

  Los Miembros aplicarán un sistema de prórroga o de renovación para atender a las situaciones en que un marino necesite que se prorrogue o se renueve su DIM, o en que se le haya perdido este último. Esta prórroga o renovación se hará constar oportunamente en la

base electrónica de datos nacional. De rechazarse un DIM en caso de caducidad, se consultará la base electrónica de datos a fin de averiguar si el DIM ha sido prorrogado o renovado. Los marinos no deberían tener más de un DIM a la vez. La reexpedición de un DIM debería invalidar todo DIM anteriormente expedido al marino de que se trate. El sistema de reconocimiento biométrico vendrá a facilitar el nuevo registro del DIM o su nueva expedición.

- «Debería aplicarse un sistema de renovación anticipado cuando un marino sepa de antemano, atendiendo al período en que deba prestar su servicio, que no estará en condiciones de presentar su solicitud de renovación cuando llegue la fecha de caducidad.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 3.9.1.) «Mientras el solicitante sea titular de un DIM, no se le debería expedir otro DIM.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 3.9.)

  Los Miembros instaurarán un sistema de prórroga y/o renovación para atender a las situaciones en que el marino necesite que se prorrogue o se renueve su DIM. El marino podrá solicitar, en su caso, una prórroga y/o una renovación cuando no pueda presentar su solicitud de renovación en circunstancias normales. La prórroga y/o renovación de un DIM se hará constar oportunamente en la base electrónica de datos nacional. De ser rechazado un DIM por causa de caducidad, se consultará la base electrónica de datos nacional a fin de verificar si el DIM ha sido prorrogado o renovado. Los marinos sólo deberían tener un DIM a la vez. La nueva expedición de un DIM debería invalidar todo DIM previamente expedido al marino. El sistema de reconocimiento biométrico vendrá a facilitar el nuevo registro del DIM o su nueva emisión.

- «Debería aplicarse un sistema de sustitución en caso de pérdida de un DIM. Cabría expedir un documento provisional apropiado.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 3.9.3.) «Mientras el solicitante sea titular de un DIM, no se le debería expedir otro DIM.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 3.9.)

  Los Miembros instaurarán un sistema de sustitución para atender a las situaciones en que un marino haya perdido su DIM. La sustitución de un DIM se hará constar en tiempo real en la base electrónica de datos nacional. Los marinos sólo deberían tener un DIM a la vez. De expedirse nuevamente un DIM, el DIM previamente expedido al marino debería quedar invalidado. El sistema de reconocimiento biométrico vendrá a facilitar la nueva inscripción del DIM o su nueva expedición. El marino podrá instar, en su caso, un DIM de repuesto por cualquier documento provisional. Deberá devolverse el documento provisional. La base electrónica de datos nacional se actualizará oportunamente a fin de reflejar los cambios pertinentes. Sólo la autoridad expedidora del DIM original podrá expedir documentos provisionales.

- «La autoridad expedidora debería instaurar procedimientos adecuados para proteger la base de datos, en particular la obligación de realizar periódicamente copias de seguridad de la base de datos, las cuales se almacenarán en soportes informáticos conservados en un lugar seguro, fuera de los locales de la autoridad expedidora.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 4.2.1.)

  La autoridad expedidora de cada Miembro debería realizar periódicamente copias de seguridad de la base electrónica de datos que deberían almacenarse en soportes informáticos conservados en lugar seguro, fuera de los locales de la autoridad expedidora.

- La autoridad expedidora de cada Miembro debería llevar un registro de «los problemas advertidos en relación con la fiabilidad o seguridad de la base electrónica de datos, incluidas las solicitudes de información en la base de datos.» (Convenio internacional del trabajo núm. 185, anexo III, parte B, párrafo 5.6.5).

  Las bases electrónicas de datos de los Miembros cumplirán una función de comprobación que permitirá consignar los problemas que incidan en la fiabilidad o la seguridad de la base electrónica de datos (inclusive las solicitudes de información dirigidas a la base de datos).

Annex A

SID pattern-based fingerprint bar code format (normative)

The SID PDF417 2-D bar code shall have 16 data symbol columns and 40 rows, utilizing error correction level 5. The data shall be recorded using byte mode. There shall be a total of 688 bytes of data in the SID pattern-based fingerprint bar code format, described below. The seafarers' fingerprint biometric data shall be recorded using the format specified in Annex B followed immediately thereafter by a set of metadata that is both printed on the surface of the SID in text and in the bar code to support seafarer authentication. The fields shall be defined as follows:

1. Fingerprint data.
   Data for two fingerprint templates in BioAPI compliant format shall be stored as specified in Annex B.

2. Issuing authority.
   The country code of the issuing authority shall be stored as an unsigned integer in two bytes.

3. Document number.
   A text stream of up to nine characters shall be stored in nine bytes. The stream consisting of the issuing authority and the document number shall be unique.

4. Personal identification number.
   An optional null terminated text stream of up to 14 characters shall be stored in 14 bytes. A stream of 14 null bytes may be stored instead.

5. Expiration date.
   The date of expiry shall be stored in SSE format.

6. Primary identification.
   The primary identification shall be stored using a null-terminated text stream in 20 bytes using up to 20 characters.

7. Secondary identification.
   The secondary identification shall be stored using a null-terminated text stream in 20 bytes using up to 20 characters.

8. Nationality.
   The country code representing the seafarer's nationality shall be stored as an unsigned integer in two bytes.

9. Place of birth.
   The place of birth shall be stored using a null-terminated text stream in 20 bytes using up to 20 characters.

10. Date of birth.
    The date of birth shall be stored in SSE format.

11. Gender.
    The gender of the seafarer shall be stored using a character "m" (0x6D) or "f" (0x66) or "x" (0x78).

12. Date of issue.
    The date of issue shall be stored in SSE format.

13. Place of issue.
    The place of issue shall be stored using a null-terminated text stream in 20 bytes.

Pattern-based fingerprint SID bar code format (informative)

Field	Size	Comments
Fingerprint data	568 bytes	See Annex B
Issuing authority	2 bytes	Country code (see note 1)
Document number	9 bytes	Text (see note 1)
Personal identification number	14 bytes	Optional text
Expiry date	4 bytes	SSE
Primary identifier	20 bytes	Text
Secondary identifier	20 bytes	Text
Nationality	2 bytes	Country code
Place of birth	20 bytes	Text
Date of birth	4 bytes	SSE
Gender	1 byte	“m” (0x6D) or “f” (0x66) or “x” (0x78).
Date of issue	4 bytes	SSE
Place of issue	20 bytes	Text

Note 1: The issuing authority plus the document number comprise the unique document identifier.

Annex B

SID bar code pattern-based fingerprint storage format (normative)

The SID bar code will be generated in a fixed format to support international interoperability. Data for two pattern-based fingerprints will be stored in a fixed-size PDF417 bar code structure in accordance with ISO/IEC 15438:2001 that uses the draft ISO/IEC pattern-based fingerprint interchange format (ISO/IEC WD 19794-3 (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003)) to encode two fingerprints with 14 cells in the X-direction, 16 cells in the Y-direction, and 3 bits each for angle, wavelength, and phase offset storage, wrapped inside a BioAPI template as outlined in the table below.

Because this fingerprint storage format was developed in accordance with draft ISO standard documents, *this document will take precedence for the seafarers' ID* should evolution of either of these draft standards create any perceived inconsistency. Copies of the two draft conformance standards; namely, ISO WD 19794-3 [12] – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003) and ISO WD 19794-4 – Biometric data interchange formats – Part 4: Finger image-based interchange format (ISO/IEC JTC 1 SC37 N 341, dated 7 October 2003), are provided in Annex C and Annex D, respectively.

Many values will be the same for every template, as indicated below. Refer to Annex C for encoding details. In no event shall an optional field be skipped. All fields marked as "Fixed" shall not contain values other than those present. Some fields are "RIU" – Reserved for implementers use. To assist in implementation, many field names from the BioAPI standard are used here.

The format is defined as follows, with an informative summary table at the end.

All values are stored without field delineators. Indexing is by byte-count. Hexadecimal notation is used unless otherwise noted.

1. The BioAPI header value shall be 16 bytes long and be 0x00002380104010103 01nn0200000008 – where nn is the signed integer with the value of 1 through 100 corresponding to the overall quality of these fingerprints.
2. After the BioAPI header comes the opaque biometric data, in this case the finger pattern-based template format as defined in Annex C (ISO/IEC WD 19794-3 (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003)).
3. At the start of the finger pattern-based template is a header. The following values shall be fixed:
   (a) the "version number" field value shall be 0x20303100 corresponding to version 0.1;
   (b) the "length of record" field value shall be 0x00000228 corresponding to 552 bytes (the "opaque biometric data", which encompasses 1st and 2nd fingerprint and finger pattern data given in informative table below);
   (c) the "number of finger patterns in record" field value shall be 0x01 corresponding to the storage of two fingerprints;
   (d) the "number of cells in X-direction" field value shall be 0x0E;
   (e) the "number of cells in Y-direction" field value shall be 0x10;
   (f) the "bit-depth of cell structure angle" field value shall be 0x03;
   (g) the "bit-depth of cell structure wavelength" field value shall be 0x03;
   (h) the "bit-depth of cell structure phase offset" field value shall be 0x03;
   (i) the "bit-depth of cell structure quality" field value shall be 0x03;

[12] ANSI/INCITS has just announced formalization of this standard under the title ANSI/INCITS 377 – Finger pattern-based interchange format.

(j) the “cell quality granularity” field value shall be 0x06;

(k) the “reserved bytes” field value shall be 0x0000.

4. After the pattern-based fingerprint template header are the two fingerprint templates themselves. A header prefixes each fingerprint template. The following values shall be fixed:

(a) the “finger location” fields shall contain a value no less than 0x01 and no greater than 0x0A. The value shall correspond to the finger stored. See section 5.1.1 for finger order preference. The values are as follows: 0x01 = Right thumb; 0x02 = Right index finger; 0x03 = Right middle finger; 0x04 = Right ring finger; 0x05 = Right little finger; 0x06 = Left thumb; 0x07 = Left index finger; 0x08 = Left middle finger; 0x09 = Left ring finger; 0x0A = Left little finger;

(b) the “impression type” field value shall be either 0x00 (corresponding to a “Live-scan plain”) or 0x08 (corresponding to “Swipe”);

(c) the “number of views in fingerprint record” field value shall be 0x00 corresponding to one view;

(d) the “length of data block in bytes” field value shall be 0x00FE corresponding to 254 bytes;

(e) the “view number” field value shall be 0x00 corresponding to the first (and only) view of this finger on this card;

(f) the “cell quality data” field value shall be 0xFF.

5. All unspecified fields are governed by Annex C (ISO/IEC WD 19694-2 (dated 8 September 2003)).

SID pattern-based fingerprint bar code storage format (informative)

Field	Size	Value	Comment
BioAPI_BIR (Biometric identification record)			
BioAPI_BIR_HEADER			
Length in bytes	4 bytes	0x00000238	Fixed – 568 bytes, includes all fields in this table
BioAPI_BIR_VERSION	1 byte	0x01	Fixed
BioAPI_BIR_DATA_TYPE	1 byte	0x04	Fixed – “Processed”
BioAPI_BIR_BIOMETRIC_DATA_FORMAT	4 bytes	0x01010301	Fixed – 0x0101 = JTC 1 SC37 format owner 0x0301 = Fingerprint pattern w/no extended data [1]
BioAPI_Quality	1 byte		Signed integer
BioAPI_BIR_PURPOSE	1 byte	0x02	Fixed – BioAPI_PURPOSE_IDENTIFY
BioAPI_BIR_AUTH_FACTORS	4 bytes	0x00000008	Fixed – BioAPI_FACTOR_FINGERPRINT
BioAPI “Opaque biometric data”			
Format identifier	4 bytes	0x46505200	Fixed – “FPR” 0x00
Version number	4 bytes	0x20303100	Fixed – “01” 0x00
Length of record	4 bytes	0x00000228	Fixed – 552 bytes; includes the “Opaque biometric data”, which encompasses 1st and 2nd fingerprint and finger pattern data below
Capture device ID	2 bytes		RIU

Field	Size	Value	Comment
Number of finger patterns in record	1 byte	0x01	Fixed – Two fingerprints
Resolution of finger pattern in X-direction	2 bytes		Pixels per centimetre
Resolution of finger pattern in Y-direction	2 bytes		Pixels per centimetre
Number of cells in X-direction	1 byte	0x0E	14 cells – Fixed
Number of cells in Y-direction	1 byte	0x10	16 cells – Fixed
Number of pixels in cells in X-direction	1 byte		
Number of pixels in cells in Y-direction	1 byte		
Cellular X-offset	1 byte		In pixels
Cellular Y-offset	1 byte		In pixels
Bit-depth of cell structure angle	1 byte	0x03	Fixed
Bit-depth of cell structure wavelength	1 byte	0x03	Fixed
Bit-depth of cell structure phase offset	1 byte	0x03	Fixed
Bit-depth of cell structure quality	1 byte	0x01	Fixed – Unused, here only for compatibility
Cell quality granularity	1 byte	0x06	Fixed – Unused, here only for compatibility
Reserved bytes	2 bytes	0x0000	Fixed – For future use
		1st fingerprint	
Finger location	1 byte	0x01-0x0A	0x02 = Right index finger 0x07 = Left index finger 0x01 = Right thumb 0x06 = Left thumb 0x03 = Right middle finger 0x08 = Left middle finger 0x04 = Right ring finger 0x09 = Left ring finger 0x05 = Right little finger 0x0A = Left little finger (From ANSI/NIST-ITL 1-2000, table 5) In order of preference
Impression type	1 byte	0x00 or 0x08	0x00 = Live-scan plain 0x08 = Swipe 0x09 = Reserved for future use
Number of views in fingerprint record	1 byte	0x00	Fixed – 1 view
Fingerprint pattern quality	1 byte	0x00-0x64	0-100
Length of data block in bytes	2 bytes	0x00FE	Fixed (254 bytes)
		1st finger pattern data	
View number	1 byte	0x00	Fixed
Finger pattern cell data	252 bytes		See Annex C
Cell quality data	1 byte	0xFF	Fixed – Unused

Field	Size	Value	Comment
		2nd fingerprint	
Finger location	1 byte	0x01-0x0A	0x02 = Right index finger 0x07 = Left index finger 0x01 = Right thumb 0x06 = Left thumb 0x03 = Right middle finger 0x08 = Left middle finger 0x04 = Right ring finger 0x09 = Left ring finger 0x05 = Right little finger 0x0A = Left little finger (From ANSI/NIST-ITL 1-2000, table 5) In order of preference
Impression type	1 byte	0x00 or 0x08	0x00 = Live-scan plain 0x08 = Swipe 0x09 = Reserved for future use
Number of views in fingerprint record	1 byte	0x00	Fixed 1 view
Fingerprint pattern quality	1 byte	0x00-0x64	0-100
Length of data block in bytes	2 bytes	0x00FE	Fixed (254 bytes)
		2nd finger pattern data	
View number	1 byte	0x00	Fixed – 1 view
Finger pattern cell data	252 bytes		See Annex C
Cell quality data	1 byte	0xFF	Fixed unused

[1] To identify that this is the same format as ISO/IEC WD 19794-3. Note, the version number (0.1) indicates that there may be differences between this standard and what the final international standard may be.

Anexo C

ISO/IEC WD 19794-3: Biometric data interchange formats

ISO/IEC JTC 1/SC 37 N313

2003-10-03

Replaces:

ISO/IEC JTC 1/SC 37
Biometrics

Document Type: Working Draft Text

Document Title: 2nd Working Draft Text for 19794-3, Biometric Data Interchange Formats - Part 3: Finger Pattern Data

Document Source: Project Editor

Project Number:

Document Status: In accordance with Rome Resolution 2.7, this document is circulated to SC 37 National Bodies for review, along with a call for technical contributions. Such contributions should be submitted to the SC 37 Secretariat by **8 December 2003**. Contributions received will be considered at the SC 37/WG 3 meeting in February in Australia.

Special Note: Recipients of this document are invited to submit notification of any relevant patent rights of which they are aware and to provide supporting documentation. This information should also be submitted to the SC 37 Secretariat by 8 December 2003.

Action ID: COM

Due Date: 2003-12-08

Distribution:

Medium:

Disk Serial No:

No. of Pages: 27

Secretariat, ISO/IEC JTC 1/SC 37, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

Reference number of working document: **ISO/IEC JTC 1/SC 37 N 313**

Date: 2003-09-08

Reference number of document: **ISO/IEC WD2 19794-3**

Committee identification: ISO/IEC JTC 1/SC 37

Secretariat: ANSI

Biometric Data Interchange Formats — Part 3: Finger Pattern Data

Élément introductif — Élément principal — Partie n: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International standard
Document subtype: if applicable
Document stage: (20) Preparation
Document language: E

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19794-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 37, *Biometrics*.

ISO/IEC 19794 consists of the following parts, under the general title Biometric Data Interchange Formats:

— *Part 1:* Framework

— *Part 2:* Finger Minutiae Data

— *Part 3:* Finger Pattern Data

— *Part 4:* Finger Image Data

— *Part 5:* Face Image Data

— *Part 6:* Iris Image Data

— *Part 7:* Signature/Sign Data

Introduction

In the interest of implementing interoperable personal biometric recognition systems, this ISO/IEC Standard establishes a data interchange format for pattern-based fingerprint recognition algorithms. Pattern-based algorithms process "global" sections of biometric images, in contrast to feature-based algorithms, which extract particular features. Pattern-based algorithms have been shown to work well with the demanding, but commercially driven, fingerprint sensor formats such as small-area and swipe sensors. Due to cost and size considerations, these small-area and swipe fingerprint sensors are desirable for deployment in portable devices such as laptops and PDA's. At the current time, there is no established mechanism for the interchange of finger pattern information for use with pattern-based fingerprint matching algorithms.

By establishing a standard for pattern-based representation of fingerprints, we:

- Allow interoperability among fingerprint recognition vendors based on a small data record.
- Support the proliferation of low-cost commercial fingerprint sensors with limited coverage, dynamic range, or resolution.
- Define a data record format that can be used with portable devices and media, such as smart cards.
- Encourage the adoption of biometrics in applications where interoperability is required.

Note that it is recommended that biometric data protection techniques in ANSI/X9 X9.84 or ISO/IEC 15408:1999 are used to safeguard the biometric data defined herein for confidentiality, integrity and availability.

Biometric data interchange formats — Part 3: Finger Pattern Based Interchange Format

1 Scope

This -standard specifies the interchange format for the exchange of pattern-based fingerprint recognition data.

2 Conformance

A biometric system or algorithm conforms to this standard if it satisfies the mandatory requirements for the generation of the finger pattern cell information as defined in section 5 and the generation of the data record as described in section 6.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANSI/INCITS 358-2002 - Information technology - BioAPI Specification

ANSI/NIST-ITL 1-2000, Standard Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo (SMT) Information

ISO/IEC CD3 19785-1.3 - Common Biometric Exchange Formats Framework (CBEFF)

ISO/IEC 15408:1999 - Evaluation criteria for IT security

4 Terms and definitions

For the purposes of this -International Standard, the following terms and definitions apply.

4.1 Biometric

A measurable, physical characteristic or personal behavioural trait used to recognize the identity of an individual.

4.2 Biometric Algorithm

A sequence of instructions used by a biometric system to process biometric information. A biometric algorithm will have a finite number of steps and is typically used by the biometric system to compute whether a biometric sample and a reference template match.

4.3 Biometric Data

Information extracted from a biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

4.4 Biometric Sample

Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).

4.5 Biometric System

An automated system capable of:

capturing a biometric sample from an end user;

extracting biometric data from that sample;

comparing the biometric data with that contained in one or more reference templates;

deciding how well they match; and

indicating whether or not an identification or verification of identity has been achieved.

4.6 Bit-Depth

The number of bits used to represent a data record parameter.

4.7 Capture

The method of taking a biometric sample from the end user.

4.8 Cell

Sub-portion of Finger Pattern (see 4.17).

4.9 Cell Structure

Structure used to represent the information contents of cell.

4.10 Cell Quality Group

The Group of Cells to which the Finger Quality parameter refers.

4.11 Comparison

The process of comparing a biometric sample with a previously stored reference template or templates.

4.12 Crop

Remove the outer regions of an image.

4.13 Dimension

Number of pixels in an acquired biometric sample image either x- or y-direction.

4.14 Down-sample

Reduce the resolution of an image by re-sampling the image. This reduces the number of pixels accordingly.

4.15 Encryption

The act of converting plaintext into cyphertext through the use of an encryption algorithm.

4.16 Enrollment

The process of collecting biometric samples from an individual and the subsequent preparation and storage of biometric reference templates.

4.17 Finger Pattern

Sub-portion and/or down-sampled version of a raw fingerprint image (see 4.22).

4.18 Finger Pattern Interchange Data

Data derived from the Finger Pattern and stored for subsequent matching with a candidate fingerprint.

4.19 Maximal Spatial Frequency

The maximal spatial frequency is the (spatial) frequency at which exactly two samples of an image span a complete period of a (co)sinusoidal pattern. This is therefore the maximal spatial frequency that can be supported by a sampling resolution, and is known as the Nyquist frequency.

4.20 Packed Data Format

Data are stored in a compacted bit form with no record separators or field tags - fields are separated by bit count only.

4.21 Pad

Embed an image in a larger array (usually filled with zeroes) to produce a resulting image of greater dimension.

4.22 Raw Fingerprint Image

Biometric sample as captured by a fingerprint sensor. This raw image will usually retain the full resolution and spatial extent permitted by the sensor.

4.23 Reference Template

Processed Biometric Data stored as representative of the user's biometric sample.

4.24 Resolution

The number of picture elements (pixels) per unit length in a sampled fingerprint image. Pixels per cm (ppcm) will be used in this standard as the units of resolution. Note that 1 dot per cm (ppcm) ≡ 2.54 pixels per inch (ppi).

4.25 Template Size

The amount of computer (or storage medium) memory taken up by the biometric reference template.

5 Finger Pattern Interchange Data

5.1 Overview

This ISO/IEC standard for finger pattern interchange data is based on:

1) conversion of the raw fingerprint image to a cropped and down-sampled finger pattern, followed by;

2) cellular representation of the finger pattern image to create the finger pattern interchange data.

5.2 Step 1) Reduction in resolution

Pattern based fingerprint algorithms require less image resolution than is traditionally provided by sensors. Therefore, the first step in data reduction typically involves a re-sampling of the data to a lower resolution. If the data are re-sampled, this should be to a resolution of no less than 78.8 ppcm (200 ppi).

5.3 Step 2) Cellular Representation

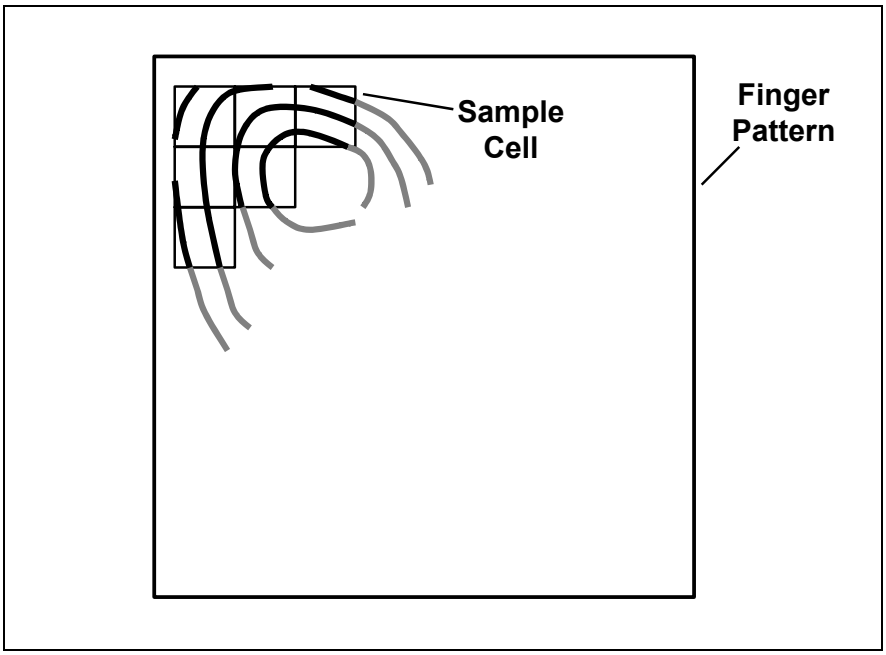


Figure 1. Diagram to illustrate Cellular Representation of Finger Pattern.

Cellular representation of the finger pattern data comprises dividing the central, or other, portion of the finger pattern into a grid of cells. At each cell the finger pattern will be represented by one of a number of different cell structures, as described below.

5.3.1 Cell Structure

Each of the candidate cell structures for representing the local finger pattern data at each cell is defined by a two-dimensional cosinusoidal pattern (see figures 2 and 3). As such, each structure is defined by three parameters; the ridge angle, θ, the ridge spacing, λ, and the phase offset, δ, as illustrated in figure 2 b).

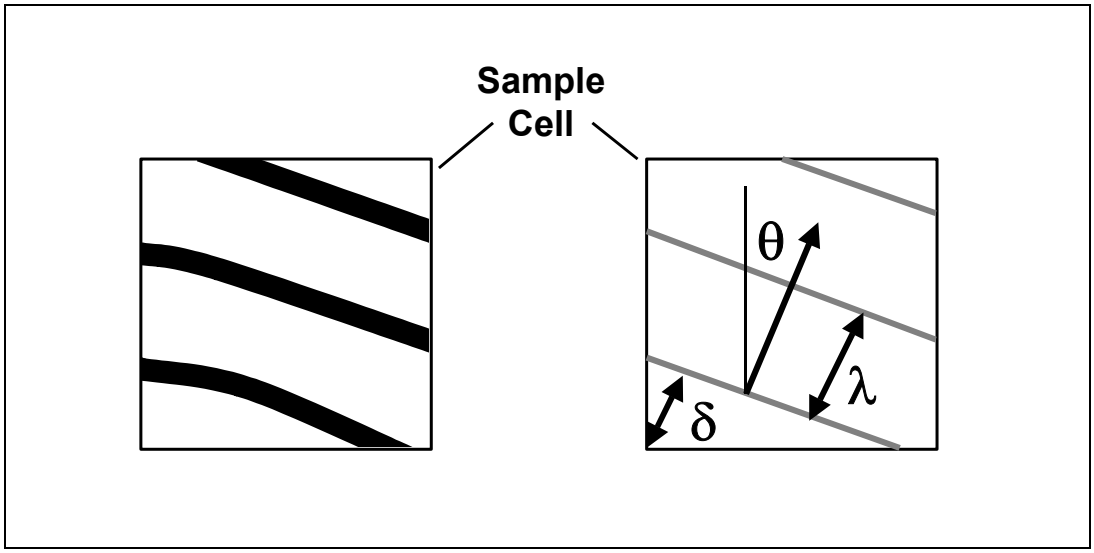


Figure 2. Cellular Representation of Finger Pattern.

The range of each of these parameters is given below:

θ: 0 to 180 degrees (where 0 degrees is defined as parallel to the y, or vertical, axis)

λ: 0 to Maximal Spatial Frequency

δ: 0 to 360 degrees

Figure 3 below demonstrates an example of a finger pattern cell a) and the resulting cell structure that is chosen to represent it b). Both of the images in this figure were enhanced for illustrative purposes.

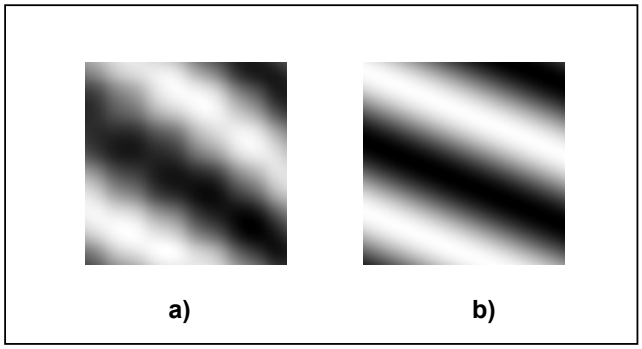


Figure 3. a) Example of the local finger pattern information in a cell, and b) the resulting cell structure chosen for representation.

In this manner, each of the finger pattern cells is represented by one of the possible permutations of cell structure. The resulting data will comprise the majority of the public portion of the Finger Pattern Data Record.

5.4 Quality

For each group of cells defined above, a quality parameter provides an indication of the quality of the information in that group of cells, with higher numbers indicating better quality. A quality granularity parameter will specify the number of cells in a Cell Quality Group: for example a value of 1 indicates a group comprises 1x1 cells; and a value of 2 indicates that a group comprises 2x2 cells. Some factors that contribute to the quality of the finger pattern cell information are gray scale resolution, gray scale linearity, spatial distortions, and location of the finger core within the raw fingerprint image.

6 Finger Pattern Data Record

6.1 Introduction

The finger pattern record format is used to provide interoperability between pattern-based fingerprint recognition systems. The record format contains both public and extended (proprietary) finger pattern interchange data. With the exception of the Format Identifier and the Version number for the standard, which are null-terminated ASCII character strings, all data is represented in binary format. There are no record separators or field tags; fields are parsed by byte count.

The biometric data record specified in this standard shall be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB).

The BDB_PID shall be defined by CBEFF.

The CBEFF BDB_biometric_organization shall be assigned by the International Biometric Industry Association (IBIA) to JTC 1 SC 37 shall be used. This is the sixteen bit value 0x0101 (hexadecimal 101 or decimal 257).

There are two different CBEFF BDB_format codes codes assigned to this standard: one for a record without an extended data portion, and one for a format with the extended data portion. If the record has no extended data, the associated CBEFF BDB_format shall be the sixteen-bit value 0x0301; if the record has an extended area, the associated CBEFF BDB_format shall be the sixteen-bit value 0x0302.

The organization of the record is as follows:

A fixed-length (32 bytes) Record Header containing information about the overall record, including the number of fingers represented and the overall record length in bytes;

A single Finger Pattern Record for each finger, consisting of:

Fixed length header (6 bytes) containing information about the data for a single finger

Finger pattern interchange data block (the block of cell data is followed by a block of quality data).

Extended data block - containing vendor-specific data.

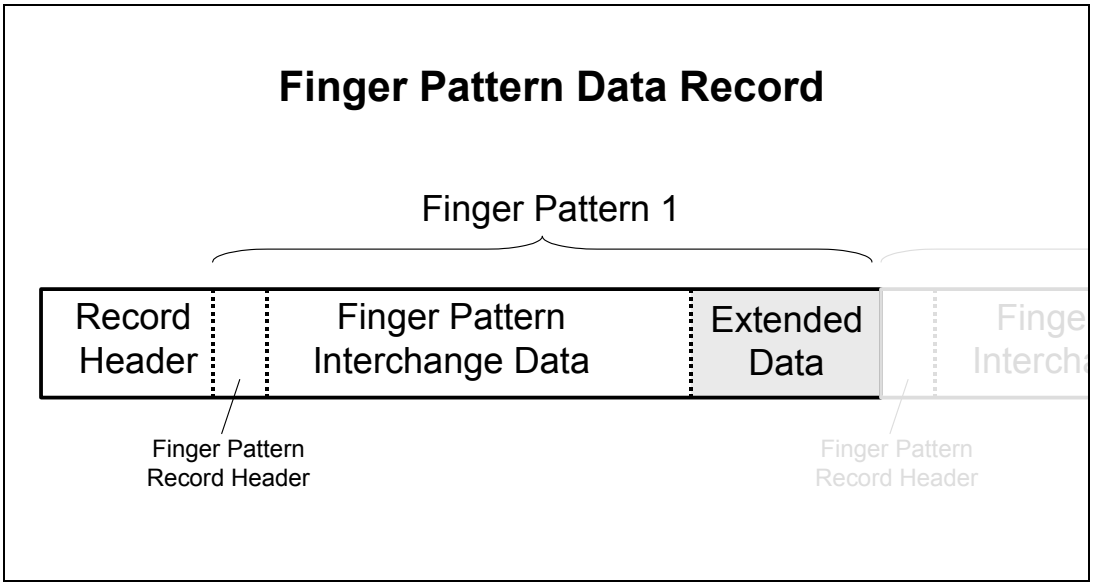


Figure 4. Diagram of Finger Pattern Data Record

All multi-byte quantities are represented in Big-Endian format; that is, the more significant bytes of any multi-byte quantity are stored at lower addresses in memory than (and are transmitted before) less significant bytes. All numeric values are fixed-length integer quantities, and are unsigned quantities.

6.2 Record Header

There shall be one and only one record header for the finger pattern record, to hold information describing the identity and characteristics of device that generated the data.

6.2.1 Format Identifier

For this standard, the Format Identifier shall consist of three characters "FPR" followed by the null character (0x0).

6.2.2 Version Number

The version number for the version of this standard used in constructing the pattern record shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major revision number and the third character will represent the minor revision number. Upon approval of this specification, the version number shall be " 10" (an ASCII space followed by an ASCII '1' and an ASCII '0').

6.2.3 Length of Record

The length of the entire record shall be recorded in four bytes.

6.2.4 Capture Device ID

The Capture Device ID shall be recorded in two bytes. A value of all zeros will be acceptable and will indicate that the Capture Device ID is unreported.

6.2.5 Number of Finger Patterns in Record

The total number of finger patterns in the record shall be contained in 1 byte.

6.2.6 Resolution of Finger Pattern in x-direction

The resolution (in ppcm) of the finger pattern(s) in the x-direction shall be record in 2 bytes. The stored valued shall be ROUND(ppcm).

6.2.7 Resolution of Finger Pattern in y-direction

The resolution (in ppcm) of the finger pattern(s) in the y-direction shall be record in 2 bytes. The stored valued shall be ROUND(ppcm).

6.2.8 Number of Cells in x-direction

The number of finger pattern cells in the x-direction shall be recorded in 1 byte.

6.2.9 Number of Cells in y-direction

The number of finger pattern cells in the y-direction shall be recorded in 1 byte.

6.2.10 Number of Pixels in Cells in x-direction

The number of pixels in the x-direction of each cell shall be recorded in 1 byte.

6.2.11 Number of Pixels in Cells in y-direction

The number of pixels in the y-direction of each cell shall be recorded in 1 byte.

6.2.12 Cellular x-offset

The number of pixels in the x-direction of the finger pattern before the first cell shall be recorded in 1 byte.

6.2.13 Cellular y-offset

The number of pixels in the y-direction of the finger pattern before the first cell shall be recorded in 1 byte.

6.2.14 Bit-depth of Cell Structure Angle

The bit-depth used to represent the Cell Structure Angle shall be recorded in 1 byte.

6.2.15 Bit-depth of Cell Structure Wavelength

The bit-depth used to represent the Cell Structure Wavelength shall be recorded in 1 byte.

6.2.16 Bit-depth of Cell Structure Phase Offset

The bit-depth used to represent the Cell Structure Phase Offset shall be recorded in 1 byte.

6.2.17 Bit-depth of Cell Structure Quality

The bit-depth used to represent the Cell Structure Quality shall be recorded in 1 byte.

6.2.18 Cell Quality Granularity

The granularity of the cell quality shall be recorded in 1 byte. The granularity is calculated as SQRT(Number of Cells in Cell Quality Group).

6.2.19 Reserved Bytes

Two bytes are reserved for future revision of this specification. For Version 1.0 of this standard, these byte values must be set to 0.

6.3 Single Finger Pattern Record Format

6.3.1 Finger Pattern Record Header

A finger header shall start each section of finger data providing information for that finger. There shall be one finger header for each finger contained in the finger pattern record. The finger header will occupy a total of six bytes as described below.

6.3.1.1 Finger Location

The finger location shall be recorded in one byte. The codes for this byte shall be as defined in Table 5 of ANSI/NIST-ITL 1-2000, "Data Format for the Interchange of Fingerprint Information". This table is reproduced here in Table 1 for convenience. Only codes 0 through 10 shall be used; the "plain" codes are not relevant for this standard.

Table 1 - Finger Location Codes

Finger location	Code
Unknown finger	0
Right thumb	1
Right index finger	2
Right middle finger	3
Right ring finger	4
Right little finger	5
Left thumb	6
Left index finger	7
Left middle finger	8
Left ring finger	9
Left little finger	10
Plain right thumb	*11*
Plain left thumb	*12*
Plain right four	*13*
Plain left four fingers	*14*

6.3.1.2 Impression type

The impression type of the finger image(s) shall be recorded in this one byte field. Nonlive entries refer to images scanned from cards or other media. These codes are compatible with Table 4 of ANSI/NIST-ITL 1-200, "Data Format for the Interchange of fingerprint Information", with the addition of the "swipe" type. The swipe type identifies templates derived from the image streams generated by sliding the finger linearly across a small sensor surface. Only codes 0 through 3 and 8 shall be used; the "latent" codes are not relevant for this standard.

Table 2 - Finger impression type

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3
Latent impression	4
Latent tracing	5
Latent photo	6
Latent lift	7
Swipe	8
Reserved	9

6.3.1.3 Number of Views in Finger Pattern

Some systems may have more than one finger record for the same finger. Each of these records represents a different view of the finger. The total number of views within each Finger Pattern Record shall be recorded in 1 byte.

6.3.1.4 Finger Pattern Quality

The quality of the overall finger pattern shall be between 0 and 100 and recorded in one byte. This quality number is an overall expression of the quality of the finger pattern. A value of 0 shall represent the lowest possible quality and the value 100 shall represent the higher possible quality. The numeric values in this field will be set in accordance with the general guidelines contained in Section 2.1.42 of ANSI/INCITS 358-2002, "BioAPI H-Level Specification Version 1.1". Further, a quality value of 101 indicates that the raw image from which the finger pattern was derived complied with Appendix F of the

Electronic Fingerprint Transmission Specification http://www.fbi.gov/hq/cjisd/iafis/efts_70.pdf).

6.3.1.5 Length of Data Block

The total length of the finger data block (including the extended data) shall be contained in 2 bytes.

6.3.2 Finger Pattern Data

6.3.2.1 Finger Pattern Interchange Data

6.3.2.1.1 View Number

Preceding the Finger Pattern Cell Data is the View Number, which is a number starting from 0 that sequentially identifies each of the views of a finger contained in this finger pattern record. The view number shall be recorded in 1 byte.

6.3.2.1.2 Finger Pattern Cell Data

The Finger Pattern Cell Data shall be stored in a packed format with the data corresponding to the upper left cell stored first, followed by the cell on left of this first cell, and so on until the first row and then subsequent rows are stored.

6.3.2.1.3 Cell Quality Data

The Cell Quality Data shall follow the Finger Pattern Cell Data and shall be stored in an identical manner, starting with the upper left value.

6.3.2.2 Finger Pattern Extended Data

This section of the Record is reserved for any proprietary data used by a System Vendor.

Table 3. Summary of Finger Pattern Data Record

Record Header			
Field	Size	Valid values	Reference
Format Identifier	4 bytes	0x46505200 ('F 'P 'R 0x0)	6.2.1
Version Number	4 bytes		6.2.2
Length of Record	4 bytes		6.2.3
Capture Device ID	2 bytes		6.2.4
Number of Finger Patterns in Record	1 byte	1-255	6.2.5
Resolution of finger pattern in x-direction ROUND(ppcm)	2 bytes	1-788	6.2.6

Resolution of finger pattern in y-direction ROUND(ppcm)	2 bytes	1-788	6.2.7
Number of Cells in x-direction	1 byte	1-(size of finger pattern in x-direction)	6.2.8
Number of Cells in y-direction	1 byte	1-(size of finger pattern in y-direction)	6.2.9
Number of Pixels in Cells in x-direction	1 byte	1-(size of finger pattern in x-direction)	6.2.10
Number of Pixels in Cells in y-direction	1 byte	1-(size of finger pattern in y-direction)	6.2.11
Cellular x-offset	1 byte	0 - (size of finger pattern in x-direction)	6.2.12
Cellular y-offset	1 byte	0 - (size of finger pattern in y-direction)	6.2.13
Bit-depth of Cell Structure Angle	1 byte	1-8	6.2.14
Bit-depth of Cell Structure Wavelength	1 byte	1-8	6.2.15
Bit-depth of Cell Structure Phase Offset	1 byte	1-8	6.2.16
Bit-depth of Cell Structure Quality	1 byte	1-8	6.2.17
Cell Quality Granularity	1 byte	1-8	6.2.18
Reserved Bytes	2 bytes		6.2.19
Finger Pattern Record Header			
Field	Size	Values	Reference
Finger Location	1 byte	0-11	Table 1
Impression Type	1 byte	0-5	Table 2
Number of Views in Finger Pattern Record	1 byte	0-255	6.3.1.3
Fingerprint Pattern Quality	1 byte	0-100	6.3.1.4
Length of data block (in bytes) including extended data	2 bytes		6.3.1.5

Finger Pattern Data			
Field	Size	Content	Reference
View Number	1 byte		6.3.2.1.1
Finger Pattern Cell Data			6.3.2.1.2
Cell Quality Data			6.3.2.1.3
Finger Pattern Extended Data			6.3.2.2

Annex A (informative) - Finger Pattern Data Record Example

This informative annex provides an example of finger pattern interchange data.

A.1 Reduction in Resolution

An example of a re-sampled image is shown below in figure 5, where an original 128x128 image, sampled at 98.5 ppcm (250 ppi), is first cropped to 120x120 pixels and then re-sampled to 78.8 ppcm (200 ppi), to produce an image of dimensions 96x96 pixels.

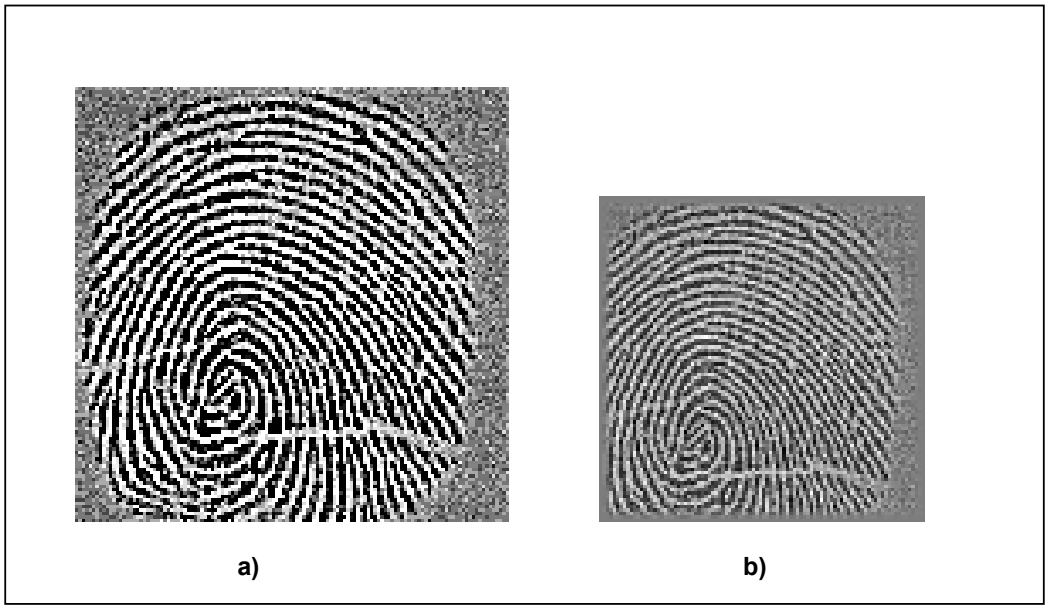


Figure 5. a) original 128x128 image sampled at 98.5 ppcm (250 ppi). b) resulting image after cropping image in a) to 120x120 pixels, and re-sampling image at 78.8 ppcm (200 ppi), to produce a 96x96 pixel dimensioned array.

A.2 Cellular Representation

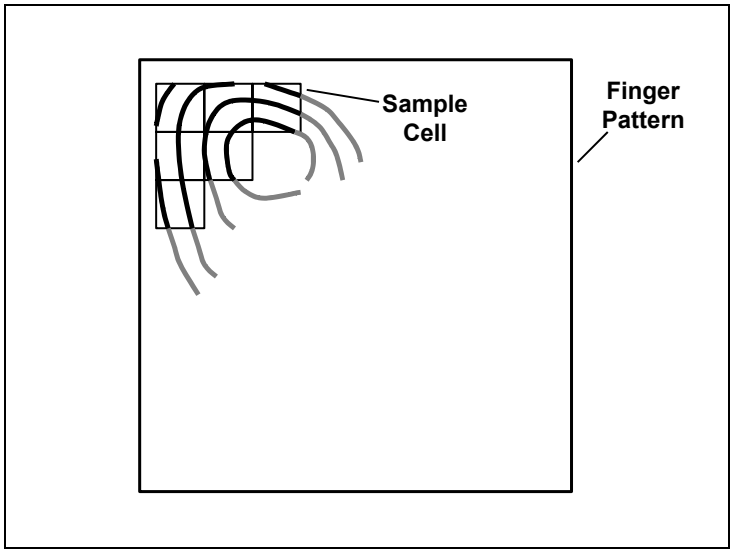


Figure 6. Diagram to illustrate Cellular Representation of Finger Pattern.

In this example, the cellular representation of the finger pattern data comprises dividing the central portion (at an offset of 13 pixels in the x-direction and 8 pixels in the y-direction) of the finger pattern into a grid of cells of dimension 5x5 pixels. Therefore, the cellular representation grid contains 14x16 cells, which represents an image area of 70x80 pixels, or 8.9x10.1 mm. At each cell the finger pattern will be represented by one of 1024 different cell structures, as described below.

A.3 Cell Structure

Each of the candidate cell structures for representing the local finger pattern data at each cell is defined by a two-dimensional cosinusoidal pattern (see figures 7).

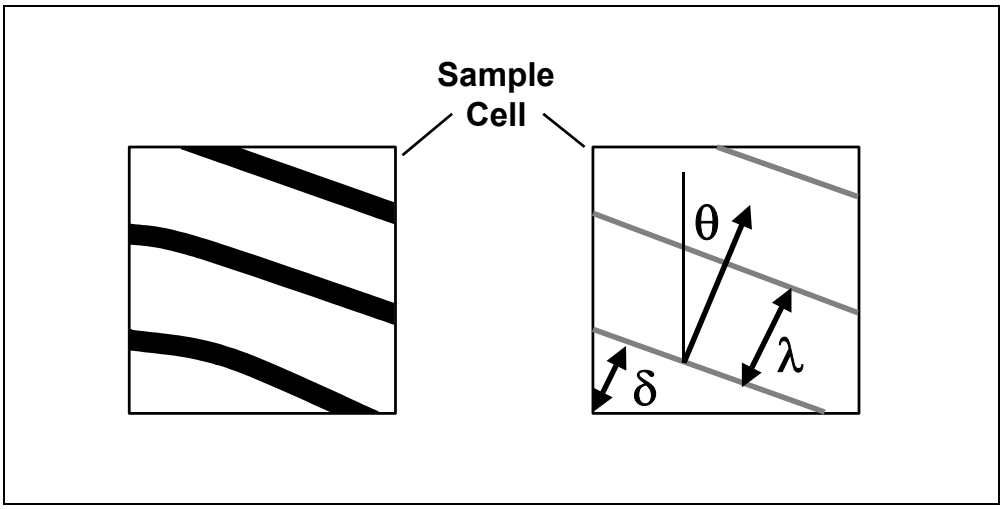


Figure 7. Cellular Representation of Finger Pattern.

The range and resolution of each of these parameters for this example is given below:

θ: 0 to 180 degrees (16 equal increments - i.e. 4 bits of information).

λ: 0 to 7/8 of the Maximal Spatial Frequency (8 increments - i.e. 3 bits of information). Therefore, for this 78.8 ppcm (200 ppi) example, a spatial frequency of 0 to 3.4 line pairs per mm is represented).

δ: 0 to 315 degrees (8 equal increments - i.e. 3 bits of information).

In this example, each of the finger pattern cells is represented by the most similar of the 1024 (16x8x8) permutations of cell structure. Therefore, each cell structure requires 10 bits of data storage (reduced from 5x5x8 bits = 200 bits per cell).

In this manner, each of the finger pattern cells is represented by one of the 1024 permutations of cell structure. The resulting data will comprise the majority of the public portion of the Finger Pattern Data Record. In this example, the finger pattern is represented by 14x16x10 bits (14 cells by 16 cells by 10 bits), which requires 280 bytes of storage.

A.4 Quality

A value of 2 indicates that a group comprises 2x2 cells. For the example stated here with 14x16 cells, and a quality granularity of 2 (2x2 cells), 56 quality parameter values will be required, at a bit-depth of 4, thus adding 28 bytes to the interchange data.

A.5 Data Record

For the example stated here, the data record comprises the following values and occupies a total of 347 bytes:

Table 4. Finger Pattern Data Record

Record Header		
Field	Size	Value
Format Identifier	4 bytes	0x46505200 ('F 'P 'R 0x0)
Version Number	4 bytes	
Length of Record	4 bytes	347
Capture Device ID	2 bytes	
Number of Finger Patterns in Record	1 byte	1
Image Resolution of finger pattern in x-	2 bytes	79

direction ROUND(ppcm)		
Image Resolution of finger pattern in y-direction ROUND(ppmm)	2 bytes	79
Number of Cells in x-direction	1 byte	14
Number of Cells in y-direction	1 byte	16
Number of Pixels in Cells in x-direction	1 byte	5
Number of Pixels in Cells in y-direction	1 byte	5
Cellular x-offset	1 byte	13
Cellular y-offset	1 byte	8
Bit-depth of Cell Structure Angle	1 byte	4
Bit-depth of Cell Structure Wavelength	1 byte	3
Bit-depth of Cell Structure Phase Offset	1 byte	3
Bit-depth of Cell Structure Quality	1 byte	4
Cell Quality Granularity	1 byte	2
Reserved Bytes	2 byte	
Finger Pattern Record Header		
Field	Size	Value
Finger Location	1 byte	2
Finger Impression	1 byte	0
View Number	1 byte	0
Fingerprint Pattern Quality	1 byte	80
Length of data block (in bytes) including private data	2 bytes	309

Finger Pattern Data		
Field	Size	
View Number	1 byte	0
Finger Pattern Cell Data	308 bytes	
Finger Pattern Extended Data	0 bytes	

Anexo D

ISO/IEC WD 19794-4: Biometric data interchange formats

ISO/IEC JTC 1/SC 37 N341

2003-10-07

Replaces:

ISO/IEC JTC 1/SC 37
Biometrics

Document Type: Text for CD ballot or comment

Document Title: Text of CD 19794-4, Biometric Data Interchange Formats – Part 4: Finger Image Data

Document Source: Project Editor

Project Number:

Document Status: In accordance with Rome resolution 2.1, this document is circulated to SC 37 National Bodies for CD letter ballot.

Special Note: Recipients of this document are invited to submit notification of any relevant patent rights of which they are aware and to provide supporting documentation. This information should also be submitted to the SC 37 Secretariat by January 7, 2004.

Action ID: LB

Due Date: 2004-01-07

Distribution:

Medium:

Disk Serial No:

No. of Pages: 31

Secretariat, ISO/IEC JTC 1/SC 37, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC 19794-4	
Date: **2003-10-07**	Reference number: ISO/IEC JTC 1/SC 37 **N 341**
Supersedes document	

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 37 Biometrics Secretariat: USA (ANSI)	Circulated to P- and O-members, and to technical committees and organizations in liaison for: - discussion at - comment by **- voting by (P-members only)** **2004-01-07** Please return all votes and comments in electronic form directly to the SC 37 Secretariat by the due date indicated.

ISO/IEC JTC 1/SC 37

Title: Biometric Data Interchange Formats – Part 4: Finger Image Data

Project: 1.37.19794.2

Introductory note:

As per Rome resolution 2.1, this document is circulated for CD letter ballot. Recipients of this document are invited to submit notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Address Reply to: Secretariat, ISO/IEC JTC 1/SC 37, Address: 25 West 43rd Street, New York, NY 10036
Telephone: +1-212-642-4932; Facsimile: +1 212-840-2298; E-Mail: LRAJCHEL@ANSI.org

ISO/IEC TC JTC 1/SC 37 N 341

Date: 2003-10-07

ISO/IEC CD 19794-4

ISO/IEC TC JTC 1/SC 37/WG 3

Secretariat: ANSI

Biometric Data Interchange Formats – Part 4: Finger Image Data

Élément introductif — Élément central — Partie 4: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (30) Committee
Document language: E
STD Version 2.1

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19794-4 was prepared by Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 37, *Biometrics*.

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19794-4 was prepared by Technical Committee ISO/IEC/TC JTC 1, *Information Technology Standards*, Subcommittee SC 37, *Biometrics*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

ISO/IEC 19794 consists of the following parts, under the general title *Biometric Data Interchange Formats*:

— *Part 1: Framework*

— *Part 2: Finger Minutiae Data*

— *Part 3: Finger Pattern Data*

— *Part 4: Finger Image Data*

— *Part 5: Face Image Data*

— *Part 6: Iris Image Data*

— *Part 7: Signature/Sign Data*

Introduction

In the forensic community, the capture and transmission of fingerprint images has been a common choice for the exchange of fingerprint information used by Automatic Fingerprint Identification Systems (AFIS) for the identification of individuals. However, little to no fingerprint information is being exchanged between equipment from different vendors in the biometric user verification and access community. This has been due in part to the lack of agreement between vendors on the amount and type of information to capture, the method of capture, and the information to be exchanged.

This proposed standard is intended for those applications requiring the exchange of raw or processed fingerprint images that may not necessarily be limited by the amount of resources required for data storage or transmitting time. It can be used for the exchange of scanned fingerprints containing detailed image pixel information. The standard can also be used to exchange processed fingerprint image data containing considerably fewer pixels per inch and/or a lesser number of greyscale levels. This is in contrast to the standard formats used for exchanging lists of fingerprint characteristics such as minutiae, patterns, or other variants. These formats require considerably less storage than a fingerprint image. However, by using any of these formats, information recorded in one standard format cannot be used by algorithms designed to operate with another type of information. In other words, minutiae data cannot be used by pattern matching algorithms and pattern data cannot be used by minutiae matching algorithms.

Although the minutiae, pattern, or other approaches produce different intermediate outputs, all must initially capture a reasonably high quality fingerprint image before reducing the size of the image (in bytes) or developing a list of characteristic data from the image. Use of the captured or processed image can provide interoperability among vendors relying on minutiae-based, pattern-based or other algorithms. As a result, data from the captured finger image offers the developer more freedom in choosing or combining matching algorithm technology. For example, an enrollment image may be stored on a contactless chip located on an identification document. This will allow future verification of the holder of the document with systems that rely on either minutiae based or pattern based algorithms. Establishment of an image-based representation of fingerprint information will not rely on pre-established definitions of minutiae, patterns or other types. It will provide implementers with the flexibility to accommodate images captured from dissimilar devices, varying image sizes, resolutions, and different grayscale depths. Use of the fingerprint image will allow each vendor to implement their own algorithms to determine whether two fingerprint records are from the same finger.

Biometric Data Interchange Formats – Part 4: Finger Image Data

1 Scope

This specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within a CBEFF data structure. This standard could be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas. Information compiled and formatted in accordance with this standard can be recorded on machine-readable media or may be transmitted by data communication facilities.

2 Conformance

Systems claiming conformance with this standard shall be capable of encoding and decoding finger image data and the associated parameter data used in the transmitting and/or receiving of fingerprint images as defined by this standard. At a minimum, conformance shall require the ability to capture, exchange, and compare interoperable fingerprint image information.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IAFIS-IC-0110 (V3) WSQ Gray-scale Fingerprint Image Compression Specification 1997

ANSI/NIST-ITL 1-2000 Information systems – Data Format for the Interchange of Fingerprint, Facial, and & Scar Mark & Tattoo (SMT) Information.

ISO International Standard 10918-1, Information Technology - Digital Compression and Coding of Continuous-Tone Still Images Part 1: Requirements and Guidelines. This is commonly referred to as the JPEG (Joint Photographic Experts Group) algorithm.

JPEG 2000 ISO International Standard15444, Information Technology - Digital Compression and Coding of Continuous-Tone Still Images Part 1: Requirements and Guidelines

ANSI/INCITS 358-2002 – Information Technology – BioAPI Specification

ISO/IEC CD 19785.3 Common Biometric Exchange Formats Framework (CBEFF) - Part 1: Data Element Specification

4 Terms and definitions

For the purpose of this document, the following terms and definitions.

4.1 biometric sample

Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).

4.2 capture

The method of taking a biometric sample from an end user.

4.3 core

The approximate center of a fingerprint image area.

4.4 fingerprint image area

The area of friction skin on the fleshy surface of a finger located horizontally between the two edges of the fingernail and vertically between the first joint and the tip of a finger. It contains a unique pattern of friction ridge and valley information commonly referred to as a “fingerprint”.

4.5 friction ridge

The ridges present on the skin of the finger which makes contact with an incident surface under normal touch.

4.6 grayscale

The method used to represent a continuous tone image that has only a single component or variable to represent each pixel; also referred to as monochrome or black and white.

4.7 image resolution

The number of pixels per unit distance in the interchanged image. This may be the result of processing a captured image. The original captured scanned image may have been subsampled, scaled, interpolated, or otherwise processed to produce a form for representing the ridge and valley structure areas of the fingerprint.

4.8 live capture

The process of capturing a biometric sample through an interaction between and end user and a biometric system.

4.9 pixel:

A picture element – located on an n by m matrix of picture elements, where n is the horizontal component and m is the vertical component.

4.10 plain fingerprint image

Image captured from a finger placed on a platen without any rolling movement – the center portion of a rolled image.

4.11 ppcm

Abbreviation for pixels per centimeter.

4.12 ppi

Abbreviation for pixels per inch.

4.13 ppmm

Abbreviation for pixels per millimeter.

4.14 rolled fingerprint image

Image area captured that is located between the two edges of the fingernail. Acquired using a rolling motion from one edge of the fingernail to the other.

4.15 scan resolution

The number of pixels per unit distance used by a sensor or scanning device to initially capture a fingerprint or palmprint image

4.16 transaction

A command, message, or input record that explicitly or implicitly calls for a processing action. Information contained in a transaction shall be applicable to a single subject.

4.17 valley

The area surrounding a friction ridge, which does not make contact with an incident surface under normal touch; the area of the finger image area between two friction ridges.

5 Data conventions

5.1 Byte and bit ordering

Each item of information, field, or logical record shall contain one or more bytes of data. Within a record all multibyte quantities are represented in Big-Endian format. That is, the more significant bytes of any multibyte quantity are stored at lower addresses in memory than less significant bytes. The order for transmission shall also be the most significant byte first and least significant byte last. Within a byte, the order of transmission shall be the most significant bit first and the least significant bit last. All numeric values are fixed-length unsigned integer quantities.

5.2 Scan sequence

It is not the purpose of this standard to specify the orientation of the finger (or palm), the method of scanning, or the order of scanning used to capture the image. However, each image as presented in accordance with this format standard shall appear to have been captured in an upright position and approximately horizontally centered. For each grayscale image area, the top left of the image will correspond to the top left of the finger. The data shall appear to have been scanned from left-to-right, progressing from the top to the bottom of the image. For the purpose of describing the position of each pixel within an image to be exchanged, a pair of reference axes shall be used. The origin of the axes, pixel location (0,0), shall be located at the upper left-hand corner of each image. The x-coordinate (horizontal) position shall increase positively from the origin to

the right side of the image. The y-coordinate (vertical) position shall increase positively from the origin to the bottom of the image.

6 Image requirements

Image capture requirements are dependent on various factors including the application, the available amount of raw pixel information to retain or exchange, and targeted performance metrics. As a result of these factors, specific numeric values will be associated with the image capture parameters including pixel aspect ratio, depth, and resolution. Values for the image acquisition parameters are required to be commensurate with the system and application requirements. Annex B provides a series of guidelines for selecting values for these parameters. Annex C provides the set of image quality specifications required for a certification process.

6.1 Pixel aspect ratio

For all quality levels, the finger image shall be represented using square pixels, in which the horizontal and vertical dimensions of the pixels are equal. Any difference between these two dimensions should be within 1%. That is, the ratio of horizontal to vertical pixel dimensions should be between .99 and 1. 01.

6.2 Pixel depth

The grayscale precision of the pixel data shall be specified in terms of the pixel depth or the number of bits used to represent the grayscale value of a pixel. A pixel depth of 3 provides 8 levels of grayscale; a depth of 8 provides up to 256 levels of gray. For grayscale data, a completely black pixel shall be represented by a zero. A completely white pixel shall have all of its bits of precision set to “1”. This implies that the byte containing a completely white pixel with five bits of grayscale shall have a value of “31”. A completely white pixel quantized to eight bits shall have a value of “255”, while a value of “1023” shall be used for a completely white pixel quantized to ten bits. The pixel depth may range from 1 to 16 bits.

6.3 Grayscale data

Grayscale finger image data may be stored, recorded, or transmitted in either compressed or uncompressed form. The image data portion of a record for an uncompressed grayscale image shall contain a set of raw pixel information. Using a pixel depth of 8 bits (256 grayscale levels) each pixel shall be contained in a single byte. Pixel values with a depth of less than eight bits can be stored and transmitted in a packed binary format. Increased precision for pixel values greater than 255 shall use two unsigned bytes to hold up to sixteen-bit pixels with values in the range of 0-65635. The encoding of a compressed grayscale image shall be the output of the appropriate grayscale compression algorithm specified. Upon decompression the grayscale value for each pixel shall be represented in the same manner as pixels in an uncompressed image.

6.4 Dynamic range

The image grayscale shall be encoded using the precision necessary to meet the dynamic range requirement for a specific application.

6.5 Scan resolution

Grayscale fingerprint image areas to be captured shall be acquired by an image capture device operating at a specific scanning resolution. As the resolution used in the image capture process is increased, more detailed ridge and structure information for processing becomes available. For minutiae and small feature based algorithms, use of the higher resolution enhances the detection of more closely spaced features that may not be detected using the minimum resolution.

6.6 Image resolution

The resolution of the image data formatted and recorded for interchange may be the scan resolution of the image or it may have been subsampled, scaled, interpolated, or otherwise processed to produce a form for representing the ridge and valley structure areas of the fingerprint.

6.7 Fingerprint image location

Some fingerprint matching systems perform better when the fingerprint core area is included in the image. This is particularly true of systems that use core-referenced features for indexing or matching. For such systems the fingerprint image should be located in the approximate middle of the image capture area. The image from the captured finger should be placed such that the core of the print is within 25% of the image dimension from the center pixel. This standard is designed to accommodate both plain (flat) or rolled images.

For multiple finger background checking and verification purposes, there are currently fingerprint scanner devices that will acquire images of multiple fingers during a single capture cycle. These devices are capable of capturing the plain impressions from four fingers of either hand during a single scanning. The plain impressions from two thumbs can also be captured at one time. Therefore, with three placements of the fingers on a device's scanning surface all ten fingers from an individual can be acquired in three scans – right four fingers, left four fingers, and two thumbs. For these multi-finger captures, half of the captured fingers should be located to the left of the image center and the other half of the fingers to the right of the image center.

7 Finger image record format

This standard defines the composition of the finger image record. Each record shall pertain to a single subject and shall contain an image record (consisting of one or more views) for each of one or more fingers, single image records for multiple fingers, or palms.

The biometric data record specified in this standard shall be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB). The CBEFF BDB_biometric_organization shall be assigned by the International Biometric Industry Association (IBIA) to JTC 1 SC 37 shall be used. This is the sixteen bit value 0x0101 (hexadecimal 101 or decimal 257). There is one CBEFF BDB_format code assigned to this standard. This code shall be included in the CBEFF Header. The associated sixteen-bit CBEFF BDB_format code shall have a value of 0x0401. The BDB_PID recorded shall be defined by CBEFF.

The organization of the record format is as follows:

- A single fixed-length (32-byte) general record header containing information about the overall record, including the number of finger/palm images represented and the overall record length in bytes;
- A single finger record for each finger, view, multi-finger image, or palm consisting of:
  - A fixed-length (14-byte) finger header containing information pertaining to the data for a single or multi-finger image;
  - Compressed or uncompressed image data view for a single, multi-finger, or palm image.

7.1 General record header

Table 1 lists the fields included in the general record header. As this is a fixed-length header, information must be included for each field within the header.

Table 1 — General record header

Field	Size	Valid values	Notes
Format identifier	4 bytes	0x464952 (‘F’ ‘I’ ‘R’ 0x0)	“FIR” – Finger Image Record
Version number	4 bytes	0x30313030 (‘0’ ’1’ ’0’ 0x0)	“010”
Record length	4 bytes	= 32 + Sum of the sizes of all finger records	Includes all finger views
Capture device ID	2 bytes		Vendor specified
Number of fingers/palms	1 byte	>=1	
Scale units	1 byte	1-2	cm or inch
Scan resolution (horiz)	2 bytes		
Scan resolution (vert)	2 bytes		
Image resolution (horiz)	2 bytes		Quality level dependent
Image resolution (vert)	2 bytes		Quality level dependent
Pixel depth	1 byte	1 -16 bits	2 – 65536 gray levels
Image compression Algorithm	1 byte	See Table 2	Uncompressed or algorithm used
Reserved	6 byte		For future definition

7.1.1 Format Identifier

The Format Identifier for the finger image standard record shall consist of the three ASCII characters "FIR" followed by the null character (0x0).

7.1.2 Version number

The number for the version of this standard used for constructing the image record shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major version number and the third character will represent the minor revision number. Upon approval of this specification, the version number shall be “010” – Version 1 revision 0.

7.1.3 Record length

The combined length in bytes for the entire record shall be recorded in these four bytes. This count shall be the sum of the lengths of all finger records (including all finger headers), the views for each finger, multiple finger record, and palms.

7.1.4 Capture device ID

The scanner ID shall be recorded in two bytes. A value of all zeros will be acceptable and will indicate that the scanner ID is unreported. The vendor determines the value for this field. Applications developers may obtain the values for these codes from the vendor.

7.1.5 Number of finger/palm images

The number of finger or palm images included in the record shall be recorded in one byte. Multiple fingers acquired by a single capture and contained in the same image are counted as a single finger image. The number of views are not part of the count for this field.

7.1.6 Scale units

This field shall specify the units used to describe the scanning and image resolutions of the image. A '0x01' in this field indicates pixels per inch, or a '0x02' indicates pixels per centimeter.

7.1.7 Scan resolution (horizontal)

This 2-byte field shall specify the rounded scanning resolution used in the horizontal direction. The scale units field will determine whether the value is pixels per inch or pixels per centimeter.

7.1.8 Scan resolution (vertical)

This 2-byte field shall specify the rounded scanning resolution used in the vertical direction. The scale units field will determine whether the value is pixels per inch or pixels per centimeter.

7.1.9 Image resolution (horizontal)

This 2-byte field shall specify the rounded image resolution used in the horizontal direction. The scale units field will determine whether the value is pixels per inch or pixels per centimeter.

7.1.10 Image resolution (vertical)

This 2-byte field shall specify the rounded image resolution used in the vertical direction. The scale units field will determine whether the value is pixels per inch or pixels per centimeter

7.1.11 Pixel depth

This 1-byte field shall contain the number of bits used to represent a pixel. This field shall contain an entry of '0x1' to '0x10'.

7.1.12 Image Compression algorithm

This 1-byte field shall specify the method used to record the uncompressed or compressed grayscale images. Table 2 lists the available storage options and compression algorithms that may be used. Uncompressed image data can be recorded in an unpacked or packed form. When using the unpacked option for grayscale pixels greater than eight bits, each pixel shall be recorded in a pair of bytes right justified. A certified version of the Wavelet Scalar Quantization (WSQ) method is generally used for 8-bit, 500 ppi grayscale images and should provide a 15:1 compression ratio. This will result in little visually observable degradation. The original DCT-based JPEG algorithm can also used for compressing 8-bit 500 ppi fingerprint images. Fingerprint images compressed with JPEG should be limited to a 5:1 compression ratio to ensure minimum humanly observable visual degradation of the image.

7.1.13 Reserved

Six bytes are reserved for future revisions of this standard. For this version of the standard this field shall be set to all '0x0'.

Table 2 — Compression algorithm codes

Code	Compression algorithm
1	Uncompressed – bit packed
2	Compressed – WSQ
3	Compressed – JPEG
4	Compressed – JPEG2000
5	PNG

7.2 Finger record header

A finger header shall start each section of finger data providing information for that view of a single finger image, multi-finger image, or palm. For each such image there shall be one finger header record accompanying the view of the image data. The finger header shall occupy a total of 14 bytes as described below. The compressed or uncompressed image data for that image view shall immediately follow the header portion. Subsequent image views (including the header portion) will be concatenated to the end of the previous image view. Table 3 is a list of the entries contained in the header preceding each set of finger image data.

7.2.1 Length of finger/palm data block

This four-byte field shall contain the length in bytes of the finger segment. It will specify the total number of bytes including the length of the header and the size of the compressed or uncompressed image data.

7.2.2 Finger/palm position

This 1-byte field shall contain the finger position. The codes for this byte as well as the maximum size of the recorded image are defined in Table 6 and Table 19 of the ANSI/NIST-ITL 1-2000 standard, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information". The tables are reproduced here as tables 4 and 5 for convenience. Codes 0-10 from table 4 should be used for single fingers. Codes 13 and 14 are used for the images containing four fingers from the right hand and left hand respectively. Code 15 is an additional code for accommodating the simultaneous capture of the two thumbs. Codes 11 and 12 should be avoided. Codes for palm images are found in table 5. For full palms the captured area should extend from the "wrist bracelet" through the second joint of the fingers. Similarly, the captured area of the upper palm should extend from the interdigital area through the second joint of the fingers. The lower palm will cover the area from the "wrist bracelet" through the interdigital area.

Table 3 — Finger image header record

Field	Size	Valid values	Notes
Length of finger data block (bytes)	4 bytes		Includes header, and largest image data block
Finger/palm position	1 byte	0-15; 20-36	See Table 4 and 5
Count of views	1	1-256	
View number	1	1-256	
Finger/palm image quality	1 byte	1-100	BioAPI specification
Impression type	1 byte		Table 6
Horizontal line length	2 bytes		Number of pixels per horizontal line
Vertical line length	2 bytes		Number of horizontal lines
Reserved	1 byte	_____	Byte set to '0x0'
Finger/palm image data	< $43x10^8$ bytes	_____	Compressed or uncompressed image data

Table 4 — Finger position code and maximum size

Finger position	Finger code	Max image area (mm^2)	Width		Length	
			(mm)	(in)	(mm)	(in)
Unknown	0	1745	40.6	1.6	38.1	1.5
Right thumb	1	1745	40.6	1.6	38.1	1.5
Right index finger	2	1640	40.6	1.6	38.1	1.5
Right middle finger	3	1640	40.6	1.6	38.1	1.5
Right ring finger	4	1640	40.6	1.6	38.1	1.5
Right little finger	5	1640	40.6	1.6	38.1	1.5
Left thumb	6	1745	40.6	1.6	38.1	1.5
Left index finger	7	1640	40.6	1.6	38.1	1.5
Left middle finger	8	1640	40.6	1.6	38.1	1.5
Left ring finger	9	1640	40.6	1.6	38.1	1.5
Left little finger	10	1640	40.6	1.6	38.1	1.5
Plain right thumb	11	2400	25.4	1.0	50.8	2.0
Plain left thumb	12	2400	25.4	1.0	50.8	2.0
Plain right four fingers	13	6800	81.3	3.2	50.8	2.0
Plain left four fingers	14	6800	81.3	3.2	50.8	2.0
Plain thumbs (2)	15	4800	50.8	2.0	50.8	2.0

7.2.3 Count of views

This one byte field shall contain the total number of specific views available for this finger.

7.2.4 View number

This one byte field shall contain the specific image view number associated with the finger.

7.2.5 Finger/palm image quality

The quality of the overall scanned finger/palm image shall be between 0 and 100 and recorded in one byte. A value of 0 shall represent the lowest possible quality and the value of 100 shall represent the highest possible quality. The numeric values in this field will be set in accordance with the general guidelines contained in Section 2.1.42 of ANSI/NCITS 358-2002, "BioAPI H-Level Specification Version 1.1". A matcher may use this value to determine its certainty of verification.

Table 5 — Palm codes, areas, and dimensions

Palm position	Palm code	Image area (cm^2)	Width (cm)	Width (in)	Height (cm)	Height (in)
Unknown palm	20	283.87	13.97	5.5	20.32	8.0
Right full palm	21	283.87	13.97	5.5	20.32	8.0
Right writer's palm	22	56.45	4.45	1.8	12.70	8.0
Left full palm	23	283.87	13.97	5.5	20.32	8.0
Left writer's palm	24	56.45	4.45	1.8	12.70	8.0
Right lower palm	25	195.16	13.97	5.5	13.97	8.0
Right upper palm	26	195.16	13.97	5.5	13.97	8.0
Left lower palm	27	195.16	13.97	5.5	13.97	8.0
Left upper palm	28	195.16	13.97	5.5	13.97	8.0
Right other	29	283.87	13.97	5.5	20.32	8.0
Left other	30	283.87	13.97	5.5	20.32	8.0
Right interdigital	31	106.45	13.97	5.5	7.62	3.0
Right thenar	32	77.42	7.62	3.0	10.16	4.0
Right hypothenar	33	106.45	7.62	3.0	13.97	5.5
Left interdigital	34	106.45	13.97	5.5	7.62	3.0
Left thenar	35	77.42	7.62	3.0	10.16	4.0
Left hypothenar	36	106.45	7.62	3.0	13.97	5.5

7.2.6 Impression type

The impression type of the finger or palm image shall be recorded in this one byte field. The codes for this byte shall be as defined in Table 6 of the ANSI/NIST-ITL 1-2000 standard, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information". The table has been shortened and is reproduced here in table 6 for convenience. Nonlive entries refer to images scanned from cards or other media.

7.2.7 Horizontal line length

This two-byte binary field shall be used to specify the number of pixels contained on a single horizontal line of the transmitted image.

Table 6 — Finger and palm impression types

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3
Latent	7
Swipe	8
Live-scan Contactless	9

7.2.8 Vertical line length

This two-byte binary field shall be used to specify the number of horizontal lines contained in the transmitted image.

7.2.9 Finger/palm image data

This field shall contain of the grayscale image data formatted and recorded in accordance with the image compression algorithm.

Annex A

Bibliography -- Informative Reference

IAFIS-IC-0110 (V3) WSQ Gray-scale Fingerprint Image Compression Specification 1997

Annex B

Image acquisition requirements

Image capture requirements are dependent on various factors including the application, the available amount of raw pixel information to retain or exchange, and targeted performance metrics. As a result of these factors, numeric values for specific image capture parameters will be associated with one of several combinations of image acquisition parameters settings. The choice of the image acquisition settings level should therefore be commensurate with the system and application requirements.

Table 7 lists the minimum requirements for selected image acquisition parameters as a function of the image acquisition settings level desired. A tolerance of plus or minus 1% is applicable to the minimum numeric values stated for the scan resolution and dynamic range parameters. The last column indicates compliance with established certification procedures. Values for setting levels 40 or 41 are intended for applications requiring the greatest amount of detailed information. Scanners capable of level 30 and 31 performance are currently available and are being deployed for law enforcement purposes. Level 30 or 31 applications primarily include law enforcement agencies. Both level 41 and 31 systems should be certified using these and other requirements contained in Appendix F of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F). The remaining two levels are designed for commercial access control and verification systems. The overall quality level of a biometric system will be limited to that level at which all of the minimums are met.

Table 7 — Image acquisition settings levels

Setting level	Scan resolution pixels/centimeter (ppcm)	Scan resolution pixels/inch (ppi)	Pixel depth (bits)	Dynamic range (gray levels)	Certification
10	49	125	1	2	None
20	98	250	3	5	None
30	197	500	8	80	None
31	197	500	8	220	EFTS/F
40	394	1000	8	120	None
41	394	1000	8	120	EFTS/F

Annex C

IAFIS IMAGE QUALITY SPECIFICATIONS

Department of Justice

Federal Bureau of Investigation

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

ELECTRONIC FINGERPRINT TRANSMISSION SPECIFICATION

JANUARY 1999

Prepared By:

Federal Bureau of Investigation

Criminal Justice Information Services Division

935 Pennsylvania Avenue, N.W.

Washington, D.C. 20535

APPENDIX F

IAFIS IMAGE QUALITY SPECIFICATIONS

1.0 SCOPE AND PURPOSE

These specifications apply to fingerprint scanner systems and printers that will supply fingerprint data to the Integrated Automated Fingerprint Identification System (IAFIS), and to printers and displays within the IAFIS. They provide objective criteria for insuring image quality.

Electronic images must be of sufficient quality to allow for: (I) conclusive fingerprint comparisons (identification or non-identification decision); (2) fingerprint classification; (3) automatic feature detection; and (4) overall Automated Fingerprint Identification System (AFIS) search reliability.

The fingerprint comparison process requires a high fidelity image without any banding, streaking or other visual defects. Finer detail such as pores and incipient ridges are needed since they can play an important role in the comparison. Additionally, the gray-scale dynamic range must be captured with sufficient depth to support image enhancement and restoration algorithms.

The image quality requirements have associated test procedures, which are described in the document *Test Procedures for Verifying IAFIS Scanner Image Quality Requirements*. These procedures will be used by the Government in acceptance testing to ensure compliance with the requirements, and in performance capability demonstrations as an indication of capability to perform. Equipment shall be tested to meet the requirements in normal operating modes, e.g., scanners shall not be tested at slower than normal operating speeds to meet modulation transfer function specifications. A vendor may recommend alternate testing methods.

2.0 FINGERPRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a fingerprint scanner (live scan and card scan). These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 500 pixels/inch, plus or minus 5 pixels per inch. The final output delivered image from the scanner system shall have a resolution of 500 pixels/inch, plus or minus 5 pixels per inch, and each pixel shall be gray level quantized to 8 bits. [Requirement described in the ANSI standard: *Data Format for the Interchange of Fingerprint Information*, ANSI/NIST-CSL 1-1993.]

2.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D □ 0.0007, for 0 □ X □ 0.07

D □ 0.01X, for 0.07□ X □ 1.50

where: D, X, Y are in inches and D = ∗Y - X∗

The requirement corresponds to a positional accuracy of ∀ 1% for distances between 0.07 and 1.5 inches, and a constant ∀ 0.0007 inches (1/3 pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.[1]

2.2 Modulation Transfer Function

The measured modulation transfer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm	MTF
1	.905 to 1.00
2	.797 to 1.00
3	.694 to 1.00
4	.598 to 1.00
5	.513 to 1.00
6	.437 to 1.00
8	.312 to 1.00
10	.200 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.[2]. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

(maximum - minimum) / (maximum + minimum)

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

MTF = representative image modulation / target modulation

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

---

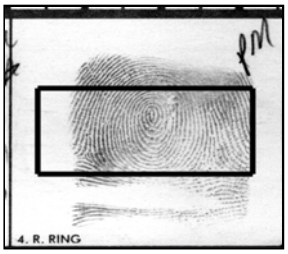
[1]Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

[2]Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

2.3 Signal-to-Noise Ratio

Both the ratio of signal to white noise standard deviation and the ratio of signal to black noise standard deviation of the digital scanner shall be greater than or equal to 125 using the following procedure:

1) A random 0.25 inch x 0.25 inch test field within the image area is chosen and the white reference target, Munsell[3] N9-white matte, is placed in the test field. 2) A white test population of 8-bit reflectance values from at least 1000 samples within the test field are collected. The average value and standard deviation are computed from this test population.



3) Steps 1 and 2 are repeated for the black reference target, Munsell N3 - black matte.

4) The signal to noise ratio (SNR) is computed as the difference between average white and average black values, alternately divided by the white noise standard deviation ('white SNR') and the black noise standard deviation ('black SNR').

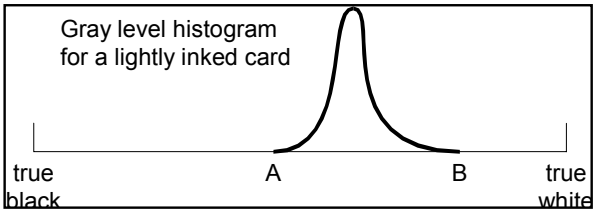
Note: The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level. Also, care should be taken, via direct visual or visual display observation, to avoid areas of dust, pinholes, scratches, or other imperfections on the target when selecting the sub-area for the 1000 samples.

2.4 Gray-Scale Range of Image Data

At least 80% of the captured individual fingerprint images shall have a gray-scale dynamic range of at least 200 gray levels and at least 99% shall have a dynamic range of at least 128 gray levels. For this requirements section, 'dynamic range' is defined as the total number of gray levels that have signal content from the fingerprint image. Fingerprint card format lines, boxes, and text shall be excluded from the dynamic range computation and white surround in the immediate vicinity of a given fingerprint shall be included in the dynamic range computation (dashed box at right). Compliance with these dynamic range requirements shall be verified using a stratified sample of fingerprint cards assembled by the Government.

[3] Munsell-Macbeth, P.O. Box 230, Newburgh, NY 12551, Phone (914) 565-7660

The intent is to avoid excessively low contrast images. Live-scan systems and card scanners at a booking station can control dynamic range by rolling the prints properly. However, with central site or file conversion systems, where a variety of card types and image qualities are encountered, adaptive processing may be necessary. The 8-bit quantization of the gray-scale values for very low contrast fingerprints needs to more optimally represent the reduced gray-scale range of such fingerprints. In the example histogram accompanying this section, the gray-scale values divide up the range from A to B. The parameters A and B are stored with the image to provide an audit trail.



2.5 Gray-scale Linearity

Using the 14 gray patches in the Sine Patterns, Inc. test target M-13-60-1X as the scanner input (independent variable), with their manufacture-supplied reflectance values, none of the corresponding 14 scanner output gray levels (dependent variable) shall deviate by more than 7.65 gray levels from a linear, least squares regression line fitted between the two variables. The output sample values within an area of at least 0.25 x 0.25 inches shall be utilized to compute the average output gray level for each patch.

2.6 Output Gray Level Uniformity

Output gray level uniformity shall be determined by scanning both a white reference target, Munsell N9 - white matte, and a black reference target, Munsell N3 - black matte. The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level in the respective tests.

Using the white target as the scanner input, the following three requirements shall be met:

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 2.5 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 22.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 12.0 gray levels.

And, using the black target as the scanner input, the following three requirements shall be met:

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 1.0 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 8.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 3.0 gray levels.

3.0 LATENT PRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a latent print scanner operating in a 1000 pixels/inch mode. These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 1000 pixels/inch. The final output delivered image from the scanner system (at the 1000 ppi setting) shall have a resolution of 1000 pixels/inch, plus or minus 10 pixels per inch, and each pixel shall be gray level quantized to a minimum of 8 bits. The complete latent print specification consists of all requirements given in this Section, plus all non-conflicting requirements given in Section 2.0 Fingerprint Scanners.

3.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between

any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

$D \leq 0.0005$, for $0 \leq X \leq 0.07$

$D \leq 0.0071X$, for $0.07 \leq X \leq 1.50$

where: D, X, Y are in inches and $D = |Y - X|$

The requirement corresponds to a positional accuracy of $\forall$ .71% for distances between 0.07 and 1.5 inches, and a constant $\forall$ 0.0005 inches (½ pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.[4]

3.2 Modulation Transfer Function

The measured modulation transfer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

[4]Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

cyc/mm	MTF
1	0.925 to 1.00
2	0.856 to 1.00
3	0.791 to 1.00
4	0.732 to 1.00
5	0.677 to 1.00
6	0.626 to 1.00
8	0.536 to 1.00
10	0.458 to 1.00
12	0.392 to 1.00
14	0.336 to 1.00
16	0.287 to 1.00
18	0.246 to 1.00
20	0.210 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.[5]. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

(maximum - minimum) / (maximum + minimum)

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

MTF = representative image modulation / target modulation

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

[5]Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

Apéndice II

Perfil biométrico creado a partir de minucias dactilares para los documentos de identidad de la gente de mar

Editores: Cynthia L. Musselman
cynthia@authenti-corp.com
Phone: 540 837 2450
Michael Crusoe
michael@authenti-corp.com
Phone: 480 889 6410

Valorie S. Valencia
valorie@authenti-corp.com
Phone: 480 889 6444

Indice

Página

Prólogo

La Organización Internacional del Trabajo, constituida en 1919, es un organismo especializado de las Naciones Unidas (NU) de carácter tripartito, en que participan en pie de igualdad representantes de los gobiernos, de los empleadores y de los trabajadores. En junio de 2003 la OIT adoptó el Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185). La revisión del antiguo Convenio, de 1958, fue motivada por una serie de debates celebrados en la Organización Marítima Internacional (OMI) y obedecía a la necesidad de reconsiderar las medidas y los procedimientos encaminados a prevenir y a evitar los actos de terrorismo que amenazan la seguridad de los buques, de sus pasajeros y de sus tripulantes. Se ha puesto el nuevo Convenio de la OIT en conocimiento de los gobiernos de los Estados Miembros de dicha organización a fin de que lo estudien con miras a su ratificación. Al ser un tratado internacional, cobrará carácter vinculante para los Miembros que lo ratifiquen.

La Oficina Internacional del Trabajo (secretaría de la Organización) encargó a las autoras del presente documento que preparasen un proyecto de informe técnico para fundamentar la elaboración de una norma que se someterá a la Organización Internacional de Normalización (ISO) con miras a su refrendo, para la adopción de una plantilla biométrica interoperable con arreglo a lo preceptuado en el Convenio núm. 185. Esta norma será aplicable a la adquisición de los datos correspondientes a huellas dactilares, a la generación de plantillas y al almacenamiento en código de barras. El informe debía versar sobre las tecnologías de impresión y de lectura más apropiadas, así como sobre los procedimientos de registro, el formato del código de barras, los captores/lectores de los datos biométricos, y las consideraciones relativas a las bases de datos y al formato de una plantilla biométrica interoperable en el mundo entero. En el informe también debían tomarse en cuenta la calidad y la interoperabilidad de las bases de datos.

La ISO y la Comisión Electrotécnica Internacional (IEC) conforman el sistema especializado de normalización mundial. Las entidades nacionales que son miembros de la ISO y de la IEC participan en la elaboración de normas internacionales a través de unas comisiones técnicas constituidas por cada entidad competente para tratar de ámbitos específicos de actividad técnica. Las comisiones técnicas de la ISO y de la IEC colaboran en campos que para ellas revisten un interés mutuo. También participan en esta labor otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con la ISO y la IEC.

Las normas internacionales se redactan atendiendo a las reglas sentadas en la parte 2 del documento ISO/IEC sobre directrices.

En lo que respecta a las tecnologías de la información, la ISO y la IEC han constituido una comisión técnica mixta, denominada ISO/IEC JTC 1. Los proyectos de normas internacionales adoptados por esta comisión técnica mixta se distribuyen a los órganos nacionales competentes para que los sometan a votación.

El presente informe fue preparado por la Oficina Internacional del Trabajo (OIT) y puede someterse a guisa de contribución técnica a la ISO/IEC JTC 1 SC37 en materia de biometría.

El presente informe, ILO SID-0002, titulado *Perfil biométrico creado a partir de minucias dactilares para los documentos de identidad de la gente de mar*, se estructura en cinco secciones, a saber:

- *Sección 1 – Ambito de aplicación*
- *Sección 2 – Cumplimiento*
- *Sección 3 – Referencias*
- *Sección 4 – Definiciones*
- *Sección 5 – Requisitos biométricos aplicables a los documentos de identidad de la gente de mar*

La sección 5, relativa a los requisitos biométricos aplicables a los documentos de identidad de la gente de mar, se subdivide a su vez en cinco apartados, a saber:

- *Sección 5.1 – Requisitos biométricos aplicables a los documentos de identidad de la gente de mar creados a partir de minucias dactilares*

- *Sección 5.2 – Requisitos aplicables al código de barras de los documentos de identidad de la gente de mar y a los lectores de estos códigos*
- *Sección 5.3 – Requisitos aplicables a la verificación de los datos biométricos en los documentos de identidad de la gente de mar*
- *Sección 5.4 – Requisitos aplicables a la base de datos de los documentos de identidad de la gente de mar*

0. Introducción

0.1. Motivos de la elaboración del documento

La Organización Internacional del Trabajo, constituida en 1919, es un organismo especializado de las Naciones Unidas (NU), con estructura tripartita, en que participan en pie de igualdad representantes de los gobiernos, de los empleadores y de los trabajadores. Tras los ataques terroristas del 11 de septiembre de 2001, la Organización Internacional del Trabajo hizo lo propio para que se revisase mediante un procedimiento acelerado el Convenio sobre los documentos de identidad de la gente de mar de 1958. El nuevo instrumento resultante, o sea, el Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185), adoptado en la reunión de la Conferencia Internacional del Trabajo de junio de 2003, permitió introducir en los documentos de identidad de la gente de mar (o «DIM») dispositivos de seguridad modernos destinados a paliar con carácter urgente el riesgo de que la gente de mar no sea admitida en el territorio de los países en que atracan sus buques con miras al disfrute de un permiso para bajar a tierra, tránsito o reembarco en otro buque. Uno de estos dispositivos de seguridad es la plantilla biométrica creada a partir de huellas dactilares, que revestirá la forma de una serie numérica impresa en un código de barras PDF417 «acorde con una norma que se elaborará posteriormente» (Convenio núm. 185, anexo 1).

En una resolución adoptada por la Conferencia Internacional del Trabajo en su reunión de junio de 2003, se pidió al Director General de la OIT que adoptase medidas urgentes «con miras a la elaboración por las instituciones competentes de una norma mundial interoperable» para la plantilla biométrica antes mencionada, especialmente en colaboración con la Organización de Aviación Civil Internacional (OACI). En una reunión celebrada en la OIT en septiembre de 2003, a la que asistieron representantes de gobiernos, armadores y gente de mar, así como de la OACI y la ISO, resultó claro que la OACI, que recomendaba una solución de reconocimiento biométrico diferente (véase más adelante) para determinar la norma aplicable a los pasaportes de lectura mecánica, no estaba en condiciones de participar activamente en la elaboración de la plantilla exigida para el nuevo DIM. También se observó que la urgencia de poner en práctica el Convenio núm. 185 obligaba a descartar los procedimientos ordinarios para elaborar dicha plantilla en el marco de la Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC).

En consecuencia, la Oficina Internacional del Trabajo encargó el presente informe técnico y pidió que en él se reflejase las exigencias contempladas en el Convenio de 2003 sobre los documentos de identidad de la gente de mar, en el cual se indican unos requisitos rigurosos para la identificación personal de la gente de mar a escala internacional a partir de información biométrica. En este informe técnico, ILO SID-0002 rev 02, las autoras presentan un perfil biométrico a fin de que sirva de norma la generación y el almacenamiento de plantillas de huellas dactilares creadas a partir de minucias en un código de barras bidimensional PDF417 en la próxima generación de DIM y en las bases de datos nacionales de los Miembros (Convenio internacional del trabajo núm. 185, anexo 1 y anexo 2, respectivamente). Este perfil biométrico se estructura de una forma casi ajustada a las normas ISO, podría materializarse en una norma e incluso, con el tiempo, en un documento de adquisición una vez que los requisitos aplicables se hayan examinado y armonizado a escala internacional.

0.2. Esfuerzos conexos

En los últimos años se han realizado varios estudios, experimentos, programas piloto y productos a fin de acelerar la inspección en los puestos fronterizos. En este empeño se procurará en gran medida incorporar tecnología de reconocimiento biométrico a la próxima generación de documentos de viaje y de documentos de identidad internacionales. Al elaborar y aprobar el

Convenio núm. 185, la Organización Internacional del Trabajo cuidó de definir los requisitos aplicables a la próxima generación de DIM, en los que se integrarán los datos biométricos de identidad de cada marino (titular del documento) y en los que se almacenarán plantillas biométricas en un código de barras.

Antes del 11 de septiembre de 2001, el sector de la biometría ya había emprendido varios proyectos de producción de normas para facilitar la elaboración de productos y sistemas interoperables de reconocimiento biométrico, así como el intercambio de datos biométricos entre productos y sistemas, y requisitos para garantizar la integridad y la confidencialidad de los datos biométricos.

- ISO/IEC FCD 19784 — tecnologías de la información — interfaz de programación de aplicación de la biometría (BioAPI) (ISO/IEC JTC 1 SC37 N, núm. 55 [1], de 17 de diciembre de 2002), en el que se presenta un interfaz de programación de aplicación que garantiza que los productos y los sistemas conformes son interoperables entre sí. (También es una norma del Instituto Nacional de Normas Estadounidense/Comisión Internacional para las Normas Relativas a las Tecnologías de la Información: ANSI/INCITS 358:2002 — tecnologías de la información — especificación BioAPI.)
- ISO/IEC CD 19785 — tecnologías de la información — marco común para los formatos de intercambio de datos biométricos (CBEFF) (ISO/IEC JTC1 SC37 N 208, de 14 de julio de 2003).
- ISO/IEC CD 19794–2 — formatos de intercambio de datos biométricos — parte 2: datos correspondientes a minucias dactilares (ISO/IEC JTC 1 SC37 N 340, de 7 de octubre de 2003).
- Norma de la Organización de Aviación Civil Internacional (OACI) sobre los documentos de viaje de lectura mecánica, encargada por la ISO/IEC JTC1 SC17.

  NB: La OACI recomendó últimamente que en la próxima generación de documentos de viaje se integre una tecnología sin contacto para tarjetas inteligentes, así como una o varias indicaciones biométricas (en virtud de la norma de la OACI sobre documentos de viaje de lectura mecánica se exigen datos biométricos faciales, y también podrían incorporarse sistemas de reconocimiento de huellas dactilares o del iris). Aunque los documentos previstos por la OIT para la gente de mar son documentos de identidad (y no documentos de viaje), la OIT procurará ajustarse en la medida de lo posible a la norma propuesta por la OACI para la próxima generación de documentos de viaje de lectura mecánica. Resulta importante destacar que en la próxima generación de DIM prevista por la OIT, los datos biométricos se almacenarán en un código de barras (en vez de un circuito integrado, como se prevé en la norma recomendada por la OACI para los documentos de viaje de lectura mecánica). Esta diferencia tiene hondas repercusiones en el perfil biométrico del DIM, pues si bien por un lado el almacenamiento en un código de barras resulta más económico que en un circuito integrado, por otro lado la capacidad de almacenamiento es mucho menor en el código de barras PDF417 para DIM que en el circuito integrado recomendado por la OACI.

En vista de que en la próxima generación de DIM prevista por la OIT se utilizará tecnología con códigos de barras para almacenar la información biométrica y contribuir al cumplimiento de los requisitos previstos por la OIT con miras a la interoperabilidad internacional de los DIM, este perfil biométrico determina el formato de almacenamiento de las plantillas de huellas dactilares en el código de barras PDF417. En consecuencia, las normas ISO/IEC 15438:2001 (símbolos de los códigos de barras PDF417) e ISO/IEC FDIS 15415 (calidad de impresión de los símbolos de los códigos de barras PDF417) son fundamentalmente aplicables a este perfil biométrico.

Combinadas, las normas ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC CD 19794-2, y el documento 9303 de la OACI, son la base sobre la cual se desarrollará el potencial biométrico de los sistemas aplicables a los DIM. Al propio tiempo, se han elaborado otras normas (como ANSI/INCITS 358:2002 — tecnologías de la información — especificación BioAPI), o se están elaborando normas nuevas, como la norma ISO/IEC WD 19794-4 — formatos de intercambio de

[1] Para averiguar el número del documento mencionado, es decir, del documento ISO/IEC JTC 1 SC37, véase en el sitio web www.jtcl.org, seleccionar subcomisión 37, buscar los documentos e introducir el número del documento en el campo «N».

datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003), que resultarán pertinentes según se indica más adelante.

0.3. Determinación de la tecnología biométrica idónea para almacenar las huellas dactilares en los documentos de identidad de la gente de mar

En el Convenio núm. 185 de la OIT se requiere que los DIM sean interoperables a escala internacional. La OIT se ve por tanto obligada a optar, respecto a la próxima generación de DIM, entre almacenar datos biométricos correspondientes a *imágenes* dactilares, a *minucias* de los dedos o bien a puntos característicos *(patrones)* de los mismos. Para fundamentar su decisión, la OIT encargó la elaboración de dos informes técnicos y se realizó una encuesta entre los Miembros de la OIT y las comunidades técnicas consultadas. En este informe, ILO SID-0002, se presentan los requisitos técnicos que se aplicarían si se adoptase la tecnología de reconocimiento biométrico basada en *minucias* dactilares, que no se ha considerado como la solución más acorde con los requisitos de aplicación para los DIM sentados por la OIT. Los motivos por los que convendría seleccionar la opción basada en ***patrones*** dactilares se exponen en el documento ILO SID-0001, rev 05, titulado *Perfil biométrico creado a partir de patrones dactilares para los documentos de identidad de la gente de mar,* y más concretamente, en la sección 5.1.4 relativa a las *Plantillas de las huellas dactilares*.

La OIT se reserva el derecho de reconsiderar esta decisión toda vez que las normas internacionales maduran y las opciones tecnológicas evolucionan, lo que también coadyuva al cumplimiento del Convenio núm. 185 de la OIT.

1. Ambito de aplicación

En la presente versión del informe técnico (ILO SID-0002), titulada *Perfil biométrico creado a partir de minucias dactilares para los documentos de identidad de la gente de mar*, se facilitan pautas de orientación para incorporar a los DIM la tecnología de reconocimiento biométrico basada en minucias dactilares, con arreglo al Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185). Las autoras del presente documento se inspiraron también en otras fuentes, a saber: 1) las notas informativas referentes a las plantillas biométricas, preparadas en la reunión oficiosa sobre la biometría al servicio de los documentos de identidad de la gente de mar, celebrada los días 29 y 30 de septiembre de 2003; 2) material de apoyo adicional; 3) la reunión de consulta técnica mantenida en Ginebra del 5 al 7 de diciembre de 2003, y 4) asesoramiento de expertos en este ámbito.

La biometría servirá para incrementar el potencial de vinculación entre los DIM y sus titulares.

El presente informe se estructura de la siguiente manera: en la sección 2 se determinan los requisitos de cumplimiento correspondientes a este perfil biométrico. En las secciones 3 y 4 se presentan respectivamente las referencias técnicas y las definiciones útiles para la lectura del presente documento. En la sección 5 se recogen los requisitos básicos que deben reunir los DIM.

Esta última sección se subdivide a su vez en cuatro apartados, a saber:

- Sección 5.1 – *Requisitos biométricos aplicables a los documentos de identidad de la gente de mar creados a partir de minucias dactilares*, relativos al registro de las huellas dactilares, a su adquisición y al formato de la plantilla en que éstas han de recogerse en la próxima generación de documentos de identidad de la gente de mar.
- Sección 5.2 – *Requisitos aplicables al código de barras de los documentos de identidad de la gente de mar y a los lectores de este código*, es decir en relación con el formato del código de barras, la tecnología y las especificaciones de impresión, la tecnología de lectura y las características físicas del código de barras.
- Sección 5.3 – *Requisitos aplicables a la verificación de los datos biométricos en los documentos de identidad de la gente de mar*, por los que se determina el procedimiento de verificación de la identidad a partir de los datos biométricos almacenados en los DIM.

- Sección 5.4 – *Requisitos aplicables a las bases de datos de los documentos e identidad de la gente de mar*, correspondientes tanto a las bases de datos de los códigos de barras como a las bases electrónicas de datos nacionales de los DIM.

En el anexo A (en inglés) se facilita una descripción pormenorizada del formato del código de barras de los DIM para huellas dactilares creadas a partir de patrones. En el anexo B se detalla el formato de almacenamiento de las huellas dactilares creadas a partir de minucias en el código de barras de los DIM. En el anexo C se reproduce el documento ISO/IEC CD 19794-2 — formatos de intercambio de datos biométricos — parte 2: datos correspondientes a minucias dactilares (ISO/IEC JTC 1 SC37 N 340, de 7 de octubre de 2003). Finalmente, en el anexo D se reproduce el documento ISO/IEC WD 19794-4 — formatos de intercambio de datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003).

En vista de que este formato de almacenamiento de huellas dactilares se elaboró de conformidad con una serie de proyectos normativos de la ISO, en el supuesto de que la evolución de alguno de dichos proyectos generase alguna incoherencia respecto a los DIM, *tendrá primacía la aplicación del presente documento*.

Se excluyen del ámbito de aplicación del presente informe técnico las cuestiones siguientes.

1) El funcionamiento general de los sistemas de identificación de la gente de mar que incluyan tecnologías biométricas.

2) Los criterios de validación de la identidad de cada marino o de su titulación profesional.

3) Los criterios de expedición de los DIM.

4) La idoneidad de tecnologías distintas de las tecnologías biométricas basadas en minucias dactilares para el programa de los DIM.

5) Los criterios aplicables a las «demás características relativas a la seguridad» mencionadas en la introducción al anexo 1 del Convenio núm. 185.

6) Las cuestiones medioambientales que revisten importancia en el entorno marítimo, como la corrosión cristalina y salina, no guardan relación con lo que es el perfil biométrico, por lo que deberían abordarse en la sección referente a las condiciones de adquisición de los DIM.

7) Valoración de riesgos en la aplicación.

2. Cumplimiento

Se considerará que los sistemas biométricos se ajustan a la presente normativa cuando cumplan correctamente todas las funciones obligatorias definidas en la sección 5, relativa a los *Requisitos biométricos aplicables a los documentos de identidad de la gente de mar,* en el anexo A, titulado SID Pattern-Based Fingerprint Barcode Format *(formato del código de barras de los DIM para huellas dactilares creadas a partir de minucias)*, y en el anexo B, titulado SID Barcode Pattern-Based Fingerprint Storage Format *(formato de almacenamiento de las huellas dactilares creadas a partir de minucias en el código de barras de los DIM).*

Cuando se preparó la presente publicación, los requisitos fijados por la OIT y la madurez de las normas internacionales aplicables a las tecnologías biométricas referentes a las huellas dactilares no permitían que se adoptase cualquier tecnología ni característica biométrica para elaborar los DIM. En la presente normativa se fijan los requisitos que habrán de permitir la interoperabilidad internacional de los componentes biométricos de las huellas dactilares creadas a partir de minucias que se almacenarán en la próxima generación de DIM.

3. Referencias

Este perfil biométrico se está elaborando antes de haberse completado los proyectos de normas atinentes a él. Los proyectos de normas mencionados en esta sección llevarán el número de registro del documento SC37 (número «n») y la fecha de publicación del proyecto indicado. En el anexo al presente documento se facilitará una copia de todos los proyectos de ***normas imperativas*** (véase sección 3.1). En vista de que el formato de almacenamiento de las huellas dactilares se elaboró conforme a proyectos normativos de la ISO, en el supuesto de que la evolución de dichos proyectos

originase alguna incoherencia respecto a los DIM, *tendrá primacía la aplicación del presente documento*.

3.1. Normas imperativas

a) ISO/IEC FCD 19784 — tecnologías de la información — interfaz de programación de aplicaciones para identificación biométrica (ISO/IEC JTC 1 SC37 N, núm. 55, de 17 de diciembre de 2002).

b) ANSI/INST-ITL 1-2000 — formato de datos para el intercambio de información sobre huellas dactilares — cuadro 5.

c) ISO/IEC FDIS 15415 — tecnologías de la información — técnicas de identificación automática y de captura de datos — especificación de prueba de calidad de impresión de los símbolos de los códigos de barra — símbolos bidimensionales.

d) ISO/IEC 15438:2001 — tecnologías de la información — técnicas de identificación automática y de captura de datos — especificaciones para los símbolos de los códigos de barras — PDF417.

e) ISO/IEC CD 19794-3 — formatos de intercambio de datos biométricos — parte 2: datos correspondientes a minucias dactilares (ISO/IEC JTC 1 SC37 N 340, de 7 de octubre de 2003).

f) ISO/IEC WD 19794-4 — formatos de intercambio de datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003).

g) ISO/IEC 8859-15:1999 — tecnologías de la información — series de caracteres gráficos codificados en un solo octeto — parte 15: alfabeto latino núm. 9.

h) ISO 3166-1:1997 — códigos para la representación de nombres de países y sus demarcaciones administrativas — parte 1: códigos nacionales.

i) ISO/IEC 9945-1:2003 — tecnologías de la información — interfaz portátil de sistemas operativos (POSIX) — parte 1: definiciones básicas.

3.2. Documentos de referencia

j) Documento 9303 de la OACI — documentos de viaje de lectura mecánica (parte 1, 5ª edición, 2003; parte 3, 2.ª edición, 2002).

k) Documento ANSI/NIST-ITL-1-2000, formato de datos normalizado para el intercambio de información correspondiente a huellas dactilares, características faciales, cicatrices y tatuajes (SMT).

l) Documento ISO/IEC 7810:2003 — tarjetas de identificación — características físicas.

3.3. Normativa y documentación adicionales que deberían elaborarse o a las que debería darse prioridad para su utilización por la gente de mar

m) Norma aplicable al perfil de aplicación para los DIM.

n) Norma de comprobación e información en materia de eficacia e interoperabiliad de los DIM.

o) Un documento de orientación adecuado y fácil de utilizar a la hora de tomar las huellas dactilares a fin de facilitar al personal encargado la tarea de registro y verificación con miras a la obtención de resultados coherentes y fiables.

4. Definiciones

Los autores han procurado velar por que los conceptos, las definiciones, los símbolos y las abreviaturas utilizados en el presente informe técnico se ajusten a la nueva norma de armonización de la terminología relativa a la biometría que está elaborando el Grupo de Trabajo 1 de la ISO/IEC JTC 1 SC 37. A continuación se facilita al lector una definición de los conceptos importantes.

4.1. Conceptos y definiciones

4.1.1. Perfil de aplicación

Series o combinaciones constitutivas de normas básicas destinadas a la realización de funciones específicas. Los perfiles de aplicación permiten determinar la utilización de opciones específicas en las normas básicas, amén de establecer una conexión entre las aplicaciones y garantizar la interoperabilidad de los sistemas.

4.1.2. Biométrico

Adjetivo. Relativo a la biometría.

NB: no debería utilizarse el vocablo «biométrico» como sustantivo.

4.1.3. Autentificación biométrica/autentificar por medios biométricos

Utilización de la verificación o la identificación biométrica para validar la autenticidad de los datos correspondientes a una persona.

4.1.4. Bloque de datos biométricos (BDB)

Bloque de datos con formato definido que contiene uno o más muestras o plantillas biométricas.

4.1.5. Identificación biométrica/identificar por medios biométricos

Asociación de una muestra biométrica a una entrada en una base de datos biométricos, contrastando la muestra biométrica con las muestras biométricas almacenadas en la base de datos, y generando índices de semejanza entre las muestras así comparadas.

4.1.6. Registro de identificación biométrica (BIR)

Estructura de datos que contiene un DBD, además de información para determinar el formato de éste y, eventualmente, indicaciones adicionales acerca de si, por ejemplo, el DBD lleva firma o codificación digital.

4.1.7. Registro de datos biométricos con fines de intercambio (BIDR)

Estructura de datos correspondientes a una persona, que contiene un BIR (véase 4.1.6) e información específica sobre los sistemas, aplicaciones y funciones de identificación de la gente de mar.

4.1.8. Muestra biométrica

Información obtenida a partir de un dispositivo biométrico, ya sea directamente o mediante un proceso determinado.

4.1.9. Verificación biométrica/verificar por medios biométricos

Confirmar que una muestra biométrica coincide con la muestra biométrica procesada, almacenada y asociada a la identidad declarada de la persona interesada, mediante un cotejo de plantillas, la generación de índices y la comparación de estos índices con el umbral de semejanza.

4.1.10. Registrar mediante procedimientos biométricos

Acopio de una o más muestras biométricas de una persona y ulterior preparación y almacenamiento de una o más muestras biométricas procesadas y de datos asociados que sean representativos de la identidad de la persona.

4.1.11. Código nacional

Código nacional numérico de tres dígitos determinado en la norma ISO 3166-1.

4.1.12. Integridad de los datos

Propiedad inherente al sistema respecto a los datos materialmente almacenados, por ejemplo, en los DIM o en la base electrónica de datos nacionales de DIM, de forma que resulte imposible alterar la información sin dejar rastros.

4.1.13. Confidencialidad de los datos

Propiedad inherente al sistema respecto a los datos materialmente almacenados, por ejemplo, en los DIM o en las bases electrónicas de datos nacionales de DIM, de forma que no puedan acceder a dichos datos ni modificarlos más que las personas debidamente autorizadas, siempre que se trate de aplicaciones accesibles a estos efectos y que se disponga del potencial tecnológico para ello.

4.1.14. Interoperabilidad mundial de los datos biométricos almacenados en los DIM

Aceptación mundial de los bloques de datos biométricos correspondientes a huellas dactilares almacenados en un código de barras bidimensional impreso en el DIM con miras a la verificación de la identidad del marino.

4.1.15. Terminado en cero

Terminado en un octeto cero (0x00).

4.1.16. Tiempo real

Vinculado o relativo a un modo de operación informática en que el ordenador recaba datos, los procesa y utiliza los resultados correspondientes para controlar los procesos mientras se producen.

4.1.17. Segundos desde la época (SSE)

Segundos desde la época (en un entero sin signo de 32 bits) del día especificado según lo dispuesto en la norma ISO/IEC 9945-1:2003, sección 4.14. Si bien se aceptan todos los segundos de cada día, cuando se desconozca el segundo exacto del día de que se trate, la aplicación del DIM se retrotraerá supletoriamente al primer segundo del mismo día.

4.1.18. Empleo del futuro

Según la práctica legislativa, el empleo del futuro designa prácticas imperativas.

4.1.19. Empleo del condicional

Según la práctica legislativa, el empleo del condicional designa prácticas recomendadas, que por ende no son obligatorias.

4.1.20. Tren textual

Tren de datos inscritos en caracteres del alfabeto latino según la norma ISO 8859-15:1999.

5. Requisitos biométricos aplicables a los documentos de identidad de la gente de mar

5.1. Requisitos biométricos aplicables a los documentos de identidad de la gente de mar creados a partir de minucias dactilares

Se imprimirán, en forma de números inscritos en un código de barras ajustado a la norma indicada en el presente documento, dos plantillas biométricas creadas a partir de minucias dactilares correspondientes al marino al que se haya expedido el documento. En el Convenio núm. 185 de la OIT se han fijado las condiciones que debe reunir el sistema resultante, las cuales se destacan a continuación. Las autoras de este perfil biométrico se han basado en la estrategia de cumplimiento.

- La huella dactilar podrá «obtenerse sin que ello implique injerencia en la privacidad del titular, molestia, riesgo para su salud, o lesión de su dignidad;» (Convenio internacional del trabajo núm. 185, artículo 3, apartado *a)* del párrafo 8).

  Con este requisito se pretende evitar que los marinos perciban la adquisición y la verificación de sus huellas dactilares como una injerencia en la privacidad y una lesión de la dignidad. Del mismo modo, los sistemas biométricos y los lectores de códigos de barra se instalarán atendiendo a criterios ergonómicos, para no incomodar a los marinos. Tanto durante la utilización de este sistema como una vez terminada ésta, se prevendrá todo riesgo para la salud. Estos sistemas se desinfectarán automáticamente al cabo de cada utilización, a fin de evitar la propagación de gérmenes que pudiera derivarse del contacto con los componentes del sistema, y a fin de que utilizar el dispositivo de adquisición de huellas dactilares no resulte más arriesgado que, por ejemplo, tocar el pomo de una puerta.

- «Los datos biométricos [serán] visibles en el documento y no [podrán] reconstituirse a partir de la plantilla o de otras representaciones;» (Convenio internacional del trabajo núm. 185, artículo 3, apartado *b)* del párrafo 8).

  Con este requisito se pretende dificultar suficientemente, a partir de los datos biométricos, la reconstitución de huellas dactilares (entiéndase «imágenes de huellas dactilares»), o la elaboración de dispositivos fraudulentos que permitan dar una representación desviada de la intención o la presencia de un marino, almacenados en el código de barras. También es necesario que los datos biométricos se consideren visibles una vez impreso el código de barras, con los datos biométricos correspondientes a la huella dactilar, en los DIM de próxima generación.

- «El material necesario para proveer y verificar [la muestra biométrica es] fácil de utilizar y, en general, asequible para los gobiernos a bajo costo;» (Convenio internacional del trabajo núm. 185, artículo 3, apartado *c)* del párrafo 8).

  Resulta claro que el requisito de fácil utilización podrán cumplirlo y, de hecho, lo cumplirán los operadores y los usuarios del sistema mediante la utilización de un sistema biométrico ergonómico. También resulta claro que la opción seleccionada por la OIT para almacenar en un código de barras datos biométricos tomados a partir de minucias dactilares atiende al requisito de «asequibilidad general para los gobiernos a bajo costo».

- «El material [utilizado] para verificar [la muestra biométrica puede] utilizarse con comodidad y fiabilidad en los puertos y en otros lugares, incluso a bordo de los buques, donde las

autoridades competentes suelen proceder a las verificaciones de identidad»; (Convenio internacional del trabajo núm. 185, artículo 3, apartado *d)* del párrafo 8).

Con este requisito se pretende que los sistemas biométricos y de lectura de tarjetas puedan utilizarse de manera fiable a bordo de los buques, en los puertos y en otros lugares, de forma que los sistemas no presenten un grado de sensibilidad inhabitual a la salinidad corrosiva, característica de dichos lugares.

- «El sistema en que se haya de [proceder a una autentificación biométrica] (con inclusión del material, las tecnologías y los procedimientos de utilización) [permitirá] obtener unos resultados uniformes y fiables en materia de autentificación de la identidad.» (Convenio internacional del trabajo núm. 185, artículo 3, apartado *e)* del párrafo 8).

  La «uniformidad» presupone que el sistema biométrico se adecue a lo previsto en el presente informe técnico en aras de la interoperabilidad y que funcionará igualmente bien para todos los marinos. También presupone que los sistemas biométricos a la venta en el mercado han de ser fiables a efectos de «autentificar la identidad» (entiéndase «verificar la identidad») para los marinos que utilicen estos sistemas.

5.1.1. Procedimiento de registro de los datos biométricos

El presente informe técnico no versa sobre la totalidad del procedimiento instaurado por la OIT para la comprobación de identidad a partir de los DIM, sino que se centra en aquella parte del procedimiento referente al registro de los datos biométricos. Todo agente habilitado para expedir DIM deberá introducir en el sistema de registro los datos personales enumerados en el anexo A. Deberá tomarse una huella del dedo índice de cada mano [2]. De faltar la yema del dedo índice o de haber sido ésta dañada hasta el punto de que no pueda producirse una huella dactilar fiable o de que ésta no se pueda registrar dada su escasa calidad, se tomará la huella de otro dedo, que puede ser un pulgar, para garantizar coherencia y eficacia operativa, y maximizar la comodidad del marino. El orden de presentación de los dedos para su registro será normalmente el siguiente:

- dedo índice de la mano derecha;
- dedo índice de la mano izquierda;
- dedo pulgar de la mano derecha;
- dedo pulgar de la mano izquierda;
- dedo corazón de la mano derecha;
- dedo corazón de la mano izquierda;
- dedo anular de la mano derecha;
- dedo anular de la mano izquierda;
- dedo meñique de la mano derecha, y
- dedo meñique de la mano izquierda.

El agente encargado de expedir los DIM especificará qué dedos se tomaron para el registro biométrico y la información quedará inscrita en el encabezamiento de la plantilla biométrica para su almacenamiento en el código de barras del DIM (véase anexo B).

En el sistema debería preverse automáticamente un índice de calidad, o bien convendría que el personal encargado del registro dispusiera de un indicador de calidad mínima aceptable para garantizar que se generen plantillas de buena calidad (recabadas o adquiridas). Deberían registrarse solamente las huellas dactilares de máxima calidad y deberían almacenarse las plantillas de estas huellas de forma que se logren resultados de comprobación fiables. El marino deberá poder

[2] Se toman las huellas dactilares de dos dedos para incrementar la fiabilidad y la eficacia del sistema. Se ha elegido el dedo índice para las huellas dactilares principales porque en la mayoría de los casos es el más fácil de colocar en el dispositivo de adquisición de huellas dactilares, para la mayor comodidad del marino (artículo 3, párrafo 8, requisito 1).

cerciorarse de que sus datos biométricos de referencia, que se almacenarán en su DIM, puedan utilizarse para facilitar la verificación biométrica, especialmente en el lugar de expedición.

El sistema de reconocimiento biométrico de las huellas dactilares deberá:

- Presentar en la pantalla indicaciones para el agente encargado de expedir los DIM y para el marino a fin de facilitar el registro. Estas indicaciones versarán sobre el procedimiento, la valoración de la calidad y la colocación adecuada de los dedos.
- Utilizar mediciones de contenido y calidad a fin de garantizar la calidad de la adquisición de las plantillas, y ofrecer la posibilidad de contrastar las medidas de contenido y calidad con los valores mínimos prefijados a fin de determinar si procede indicar al marino que vuelva a presentar el mismo dedo o el dedo siguiente para un nuevo registro.
- Efectuar una medición a fin de indicar la calidad de la plantilla de la huella dactilar adquirida y facilitar información visual al operador (agente encargado de la expedición del DIM) y a la persona que se registre (el marino) acerca de la imagen de la huella dactilar tomada.
- En el caso de que el sistema biométrico no logre adquirir una plantilla aceptable para un dedo determinado, permitir al agente encargado de la expedición del DIM proceder al registro de otro dedo.
- Permitir al marino proceder a una comprobación biométrica antes de que se imprima el código de barras de su DIM, a fin de que la plantilla adquirida corresponda a la huella dactilar registrada y sea aceptable desde un punto de vista operativo para el marino. Se indicará que los dedos corresponden (identidad comprobada) cuando el índice de semejanza supere los valores mínimos fijados para la verificación (véase 5.3.1), y se indicará que no corresponden (identidad no comprobada) cuando el índice de semejanza no supere los valores mínimos para el reconocimiento.
- Indicar el número de dedos que se haya conseguido registrar.
- Permitir al agente encargado de expedir los DIM examinar los datos textuales introducidos, modificarlos según se le haya indicado, e imprimir el código de barras del DIM.
- Corroborar el reconocimiento biométrico del marino mediante el DIM impreso con arreglo a lo indicado en la sección 5.3.1.

5.1.2. Documentación para el registro de los datos biométricos

Se facilitará al personal una documentación fácil de utilizar sobre la manera de proceder al registro a fin de que se tomen huellas dactilares de buena calidad y se almacenen en el DIM plantillas de huellas dactilares que sean igualmente de buena calidad.

5.1.3 Adquisición de las huellas dactilares

Durante el registro, el dispositivo de adquisición de huellas dactilares creará plantillas biométricas a partir de minucias dactilares con arreglo a lo previsto en el cuadro 1 del anexo A del proyecto de norma ISO/IEC WD 19794-4 — formatos de intercambio de datos biométricos — parte 4: formato de intercambio basado en imágenes dactilares (ISO/IEC JTC 1 SC37 N 341, de 7 de octubre de 2003)[3] (véase anexo D al presente documento para consultar la versión integral del proyecto de norma) con un nivel mínimo de calidad de adquisición de datos de huellas dactilares de grado 3[4], según se especifica *infra*:

[3] El Grupo de Trabajo 3 de la ISO/IEC JTC 1 SC37 está revisando este proyecto de normativa. Esperamos que los parámetros de calidad de grado 3 se mantengan cuando la norma sea aceptada. Con todo, para los DIM primarán los parámetros indicados en el presente documento.

[4] El nivel de calidad 3 para la adquisición de los datos correspondientes a las huellas dactilares es aceptable para las imágenes que hayan de utilizarse para generar plantillas de huellas dactilares a partir de patrones. Obsérvese que la calidad de la adquisición de los datos correspondientes a las

- resolución de exploración: 197 píxeles/cm (500 píxeles/pulgada)
- profundidad de píxel: 8 bits
- gama dinámica (escala de grises): 220
- certificación: EFTS/F

El dispositivo de adquisición de las huellas dactilares producirá una imagen de la huella dactilar que se centrará preferiblemente en el corazón de dicha huella. Se incluirá un máximo de 52 minucias en cada plantilla de huella dactilar. «Si el número de minucias excediese del número máximo admisible por tarjeta, sería necesario proceder a un truncamiento. El truncamiento constituye la segunda etapa del proceso. Primero se eliminan las minucias dactilares de escasa calidad. Si subsisten demasiadas minucias, se procederá a un truncamiento eliminando las minucias de la superficie convexa [5] de la serie de minucias y, a continuación, se ordenarán las minucias restantes por el orden señalado en la tarjeta» [6].

Cuando se transmita la imagen de la huella dactilar al algoritmo de extracción de la plantilla, por ejemplo desde el dispositivo de adquisición hasta el ordenador, los datos saldrán sin comprimir o serán comprimidos sin pérdida.

5.1.4. Plantillas de las huellas dactilares

El algoritmo extraerá una plantilla a partir de la imagen de la huella dactilar adquirida con arreglo a la norma ISO/IEC CD 19794-2 — formatos de intercambio de datos biométricos — parte 2: datos correspondientes a minucias dactilares (ISO/IEC JTC 1 SC37 N 340, de 7 de octubre de 2003). Las plantillas de las huellas dactilares se almacenarán en la base electrónica de datos nacionales de los Estados Miembros (base de datos del Convenio) y en el código de barras bidimensional PDF417 del DIM durante el registro. Dichas plantillas también se utilizarán para comprobar el grado de correspondencia durante la verificación.

La OIT privilegiará la utilización de la plantilla creada a partir de *minucias* dactilares para facilitar las búsquedas en las bases de datos de los gobiernos antes de la expedición del DIM, a fin de comprobar la identidad del interesado. Muchos países Miembros que contestaron a la solicitud de información cursada por la OIT en diciembre de 2003 indicaron que tenían la intención de utilizar datos correspondientes a huellas dactilares para efectuar búsquedas en las bases de datos de los gobiernos [7]. Estas bases de datos de los gobiernos son en general sistemas internacionales de información sobre huellas dactilares automatizados (IAFIS), concebidos para facilitar las búsquedas con los sistemas basados en plantillas creadas a partir de *minucias*.

- A tenor de lo dispuesto en el Convenio núm. 185, artículo 3, párrafo 8, apartado *b)*, *«los datos biométricos [entiéndase, los «datos correspondientes a las huellas dactilares almacenadas en el código de barras PDF417»] [serán] visibles en el documento y no [podrán] reconstituirse a partir de la plantilla o de otras representaciones»*.

  Los datos biométricos correspondientes al marino se almacenarán en el código de barras PDF417, el cual se imprimirá de forma visible en el DIM.

  Los datos biométricos se almacenarán en dos plantillas creadas a partir de minucias que se formatearán con arreglo a lo indicado en los anexos B y C al presente informe.

huellas dactilares es distinta e independiente de la calidad de la imagen de impresión del código de barras del DIM.

[5] La superficie convexa es la forma más pequeña (polígono) que reúne una serie de puntos.

[6] ISO/IEC CD 19794-2, de 7 de octubre de 2003 (ISO/IEC JTC 1 SC37 N 340, párrafo 8.3.1).

[7] El actual proyecto de norma de almacenamiento de datos correspondientes a las minucias no se ajusta a la norma IAFIS vigente ni a las demás normas AFIS, aunque obedece a los mismos principios e ideas. Se necesitaría un simple programa de conversión para utilizar los datos a fin de contrastarlos con los registrados en las bases de datos de los Estados Miembros.

La OIT deberá averiguar qué consecuencias tendría el hecho de imponer la plantilla fija definida en los anexos B y C. Durante estas averiguaciones que todavía están por definir, deberían valorarse las consecuencias que tendría la utilización de la plantilla de tamaño fijo en cada solución comercial y en las demás consecuencias de las múltiples soluciones comerciales. Por ahora no se ha procedido a comprobación oficial alguna para garantizar que el cumplimiento de los requisitos contemplados en el Convenio de la OIT núm. 185 no mermarán la eficacia del sistema de reconocimiento biométrico.

- En virtud de lo dispuesto en el Convenio núm. 185, artículo 3, párrafo 8, apartado *b)*, «los datos biométricos [entiéndase los «datos correspondientes a huellas dactilares almacenadas en el código de barras PDF417»] [serán] visibles en el documento y *no [podrán] reconstituirse a partir de la plantilla o de otras representaciones*».

  La evaluación de los resultados de los productos biométricos en que se utilizan minucias versarán no sólo sobre las consecuencias de la utilización de la plantilla de tamaño fijo, sino que también tendrá por objeto velar por que resulte considerablemente difícil reconstituir la imagen de una huella dactilar o elaborar dispositivos fraudulentos que puedan servir para dar una representación desviada de la intención o la presencia de un marino con la utilización de los datos almacenados en plantillas de tamaño fijo de un vendedor determinado que comprendan huellas dactilares creadas a partir de minucias [8].

De conformidad con la norma ISO/IEC CD 19794-2 — Formatos de intercambio de datos biométricos — parte 2: datos correspondientes a minucias dactilares (ISO/JTC 1 SC37 N 340, de octubre de 2003), las características de la plantilla biométrica creada a partir de minucias dactilares para los DIM previstos por la OIT se detallan en los anexos A, B y C. A continuación se resume la estructura de los datos del código de barras del DIM:

- Encabezamiento BioAPI-16 octetos.
- Encabezamiento para los datos almacenados en la plantilla de la huella dactilar creada a partir de minucias – 30 octetos.
- Dos plantillas creadas a partir de minucias dactilares – hasta 520 octetos [9].
- Representación digital de los datos con arreglo al anexo A – 120 octetos.
- Tamaño total del código de barras del DIM – hasta 686 octetos.

5.2. Requisitos aplicables al código de barras de los documentos de identidad de la gente de mar y a los lectores de estos códigos

5.2.1. Formato del código de barras

El formato del código de barras del DIM se ajustará a lo dispuesto en el anexo A. El código de barras de los DIM para huellas dactilares creadas a partir de minucias contendrá hasta 686 octetos de datos y 64 símbolos de datos para un nivel de corrección de errores de 5. El código de barras

[8] Bromba, M.: «On the reconstruction of biometric raw data from template data», 9 de julio de 2003. Cargar de la página Web: http://www.bromba.com/knowhow/temppriv.htm. Hill, C.J.; Risk of Masquerade Arising from the Storage of Biometrics, B.S. Tesis. Universidad Nacional Australiana. 2001. Cargar de la página Web: http//www.chris. fornax.net/biometrics.html.

[9] Se representarán hasta 52 minucias por dedo. En el caso de que a un dedo correspondiesen más de 52 minucias, se procedería a un truncamiento con arreglo a la norma ISO/IEC CD 19794-2, de 7 de octubre de 2003 (ISO/IEC JTC SC37 N 340, párrafo 831), en cuya virtud «si el número de minucias excediese del número máximo admisible por tarjeta, sería necesario proceder a un truncamiento. El truncamiento constituye la segunda etapa del proceso. Primero se eliminan las minucias dactilares de escasa calidad. Si subsisten demasiadas minucias, se procederá a un truncamiento eliminando las minucias de la superficie convexa de la serie de minucias y, a continuación, se ordenarían las minucias restantes por el orden señalado en la tarjeta».

contendrá la información de la plantilla biométrica, así como una información que se imprimirá sobre el DIM, a saber: la autoridad expedidora; el número de identidad personal facultativo; el nombre completo del marino; el número de documento único; la fecha de caducidad del documento; la nacionalidad del marino; la fecha y el lugar de nacimiento del marino, su sexo y el lugar y la fecha de expedición del documento (véase anexo A). Las plantillas biométricas correspondientes al marino, que admitirán dos huellas dactilares, se formatearán con arreglo a lo indicado en el anexo B, en el que se define el bloque de datos biométricos de un máximo de 566 octetos indicado en el anexo A. Este bloque de datos biométricos de un máximo de 566 octetos, sumado a la información del encabezamiento de 120 octetos descrito en el anexo A, configura el código de barras del DIM, que tiene una capacidad máxima de 686 octetos.

Se aplicará la tecnología del código de barras bidimensional PDF417 atendiendo a las consideraciones siguientes:

- que los símbolos PDF417 se ajusten a los requisitos de capacidad de almacenamiento de datos de esta aplicación;
- que los símbolos PDF417 puedan leerse con un escáner de lectura bidimensional o con escáneres normales CCD (con dispositivo de transferencia de carga) o láser y un programa informático especial de descodificación. En cambio, los escáneres de lápiz de contacto no leerán los símbolos. Esta amplia gama de productos tecnológicos de lectura de códigos de barras, asequibles y a la venta en el mercado, facilitará la verificación biométrica de la identidad de los marinos.

El tamaño y la ubicación del código de barras se ajustarán a las características preceptuadas por la Organización de Aviación Civil Internacional (OACI), en la parte 1 del documento 9303 (quinta edición, 2003) y en la parte 3 del documento 9303 (segunda edición, 2002), y según se reseña más adelante:

- para los documentos con formato de libreta, el tamaño máximo del código de barras será de 21,35 mm x 86,0 mm, incluidas las zonas de silencio, según se especifica en la parte 1 del documento 9303 de la OACI – pasaportes de lectura mecánica – IV especificaciones técnicas – sólo para los pasaportes de lectura mecánica – anexo E (normativo) empleo de códigos de barras opcionales, en la página de datos del pasaporte de lectura mecánica;
- para los DIM con formato de tarjeta, el tamaño máximo del código de barras será de 27,8 mm x 85,6 mm[10], inclusive las zonas de silencio (véase parte 3 del documento 9303 de la OACI – documentos de viaje de lectura mecánica oficiales de tamaño 1 y de tamaño 2 – anexo E (normativa) a la sección IV – empleo del código de barras opcional en el DV-1).

Además, el código de barras del DIM se ajustará a los siguientes requisitos:

- Tamaño X: la anchura mínima del módulo de símbolos será de 0,170 mm (de ser posible mayor, para rellenar la zona correspondiente de la tarjeta, hasta un tamaño máximo de 0,175 mm);
- Tamaño Y: la altura mínima de la fila será de 0,511 mm (el triple de la dimensión X, de ser posible mayor, para rellenar la zona correspondiente de la tarjeta, hasta un tamaño máximo de 0,525 mm);
- Nivel cinco de corrección de errores, según se recomienda en la norma ISO/IEC 15438:2001, anexo E, y en la parte 3 del documento 9303 de la OACI (segunda edición, 2002);
- Número de columnas de símbolos informativos = 16 [11].

[10] Ello significa que la próxima generación de DIM con formato de tarjeta será de tamaño 1 y no 2 correspondiente a los documentos de viaje de lectura mecánica, según se especifica en la parte 3 del documento 9303 de la OACI (segunda edición, 2002).

[11] El Sr. Sprague Ackley, experto de renombre internacional en tecnologías para códigos de barras bidimensionales PDF417, declara que «si bien no se sabe todavía a ciencia cierta a partir de cuándo los reproductores de imágenes bidimensionales empiezan a tener dificultades con los símbolos PDF417 con varias columnas, es casi seguro que 25 columnas de datos frustrarán el funcionamiento

- Número de filas necesario para incluir los datos (40 filas [12]).

5.2.2. Tecnología empleada en las impresoras y especificaciones de impresión

El código de barras PDF417 para DIM se imprimirá con arreglo a la norma ISO/IEC 15438:2001. Los símbolos del código de barras bidimensional PDF417 pueden imprimirse con las mejores marcas de impresoras profesionales térmicas, láser y chorro de tinta. La próxima generación de impresión de códigos de barras de gran calidad se ajustará a la norma ISO/IEC FDIS 15415 – especificación de prueba de calidad de impresión de los símbolos de los códigos de barras – símbolos bidimensionales, con la signatura 3.0/05/660. Esta signatura corresponde a la categoría genérica de 3,0 atribuida a los símbolos, resulta de una apertura de 0,125 mm y una longitud de honda de 660 nm.

Los códigos de barras de los DIM se imprimirán de forma que el documento tenga la resistencia al desgaste exigible para todo DIM.

La ubicación de la zona de impresión del código de barras se ajustará a las especificaciones de la OACI previstas en la parte 1 del documentos 9303 (quinta edición, 2003) y en la parte 3 del documento 9303 (segunda edición, 2002).

5.2.3. Tecnología de lectura

Los símbolos de los códigos de barras PDF417 para los DIM de próxima generación se leerán con un escáner bidimensional, o con escáneres clásicos CCD o láser, y con un software especial de descodificación que leerá los códigos de barras impresos con arreglo a las secciones 5.2.1 y 5.2.2. En cambio, los escáneres de lápiz de contacto no leerán los símbolos PDF417.

5.2.4. Características físicas del código de barras

La «plantilla biométrica correspondiente a la huella dactilar impresa en forma de números en un código de barras» (Convenio Internacional del Trabajo núm. 185, anexo I, párrafo 3, *k)*) «estará protegida 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» (Convenio Internacional del Trabajo núm. 185, anexo I). Esta protección mejorará también la resistencia del código de barras al tiempo.

«Los datos biométricos [serán] visibles en el documentos» (Convenio Internacional del Trabajo núm. 185, artículo 3, apartado *b)* del párrafo 8). Este requisito debe interpretarse en el sentido de que los datos biométricos se considerarán visibles cuando el código de barras en que estén almacenados los datos biométricos correspondientes a las huellas dactilares se imprima en el DIM de próxima generación. El código de barras será visible cuando esté impreso en el DIM. Además, el marino podrá ver una representación binaria de la plantilla integrada en el código de barras y verificar personalmente los datos biométricos utilizando el DIM como fuente de referencia en los puestos de expedición de dichos documentos.

de los reproductores de imágenes bidimensionales». La utilización de 16 columnas de datos (20 en total) permitirá emplear una tecnología de lectura de códigos de barras de exploración bidimensional con suficiente espacio vertical para incluir en el DIM el código de barras y los datos.

[12] La derivación del número de filas del formato del código de barras del DIM correspondiente a minucias se detalla a continuación: se prevén 686 octetos de datos en cada DIM. Cada palabra de código puede almacenar 1,2 octetos. Por tanto, hay 686/1,2 = 572 palabras de código. Se necesitan 64 palabras de código adicionales para los códigos de corrección de errores de nivel 5, además de una palabra de código para toda la extensión del código de barras. Por tanto, hay un total de 572 + 64 + 1 = 637 símbolos informativos en el código de barras de los DIM. Hay 16 columnas de datos. Por tanto, se necesitan 637/16 = 40 filas para almacenar los datos en el código de barras de los DIM.

5.3. Requisitos aplicables a la verificación de los datos biométricos en los documentos de identidad de la gente de mar

5.3.1. Procedimiento de verificación de los datos biométricos

Se explorará el código de barras del DIM con un lector especial, que leerá la información del encabezamiento y de la plantilla correspondientes. En el encabezamiento constará qué huellas dactilares están almacenadas en el código de barras.

El sistema invitará al marino a que coloque el primer dedo para la lectura de la plantilla dactilar almacenada en el código de barras.

Si el dedo correspondiente al primer dedo registrado está ocupado, está dañado o no fue captado, o si el resultado del reconocimiento no supera el valor umbral de semejanza al cabo de tres intentos, el sistema pedirá al marino que coloque el segundo dedo inscrito en el dispositivo de adquisición biométrica. Si las características del dedo explorado coincide con las plantillas correspondientes almacenadas en el código de barras, se comprobará la identidad coincidente del marino. Si ninguno de los dedos que se explore se ajustan a las plantillas correspondientes almacenadas en el código de barras, el sistema indicará que no ha conseguido comprobar la información. Si al cabo del tercer intento con los dos dedos inscritos el sistema indica que no ha conseguido verificar la información, no se permitirán más intentos con el mismo DIM sin que intervenga un miembro del personal autorizado para proceder a la comprobación.

El sistema de reconocimiento biométrico para huellas dactilares deberá:

- recuperar la plantilla del código de barras bidimensional PDF417 del DIM;
- pedir a la autoridad que verifique el DIM y al marino que coadyuve a la verificación, y facilitar indicaciones de procedimiento, información sobre la colocación adecuada de los dedos y los resultados de la verificación;
- indicar al marino que coloque el dedo apropiado en el captor de imagen;
- comparar la imagen de la huella dactilar adquirida con la plantilla correspondiente almacenada en el código de barras;
- facilitar una indicación de reconocimiento (identidad comprobada) si el resultado del reconocimiento supera el umbral de semejanza, y señalar un desajuste (identidad no comprobada) si el resultado del reconocimiento es inferior al umbral de semejanza;
- exigir la intervención del personal de verificación cuando, al cabo de tres intentos con cada dedo, el marino no consiga que se reconozca ninguno de sus dedos registrados.

El sistema biométrico para huellas dactilares debería:

- estar dotado de un umbral de semejanza tal que, tanto la tasa de falsas aceptaciones como la de falsos rechazos sean inferiores al 1 por ciento de toda la población;
- dotarse de medidas de contenido y calidad proporcionales a la calidad métrica requerida para el registro;
- ofrecer, con carácter facultativo, una medida que indique la calidad de la plantilla de la huella dactilar adquirida.

5.3.2. Documentación para la verificación de los datos biométricos

Se facilitará al personal una documentación fácil de utilizar sobre la manera de proceder a la verificación.

5.4. Requisitos aplicables a la base de datos de los documentos de identidad de la gente de mar

5.4.1. Base de datos de los códigos de barras

«Los marinos [tendrán] fácil acceso a las máquinas que les [permitirán] examinar los datos que se refieran a ellos y no puedan leerse a simple vista. Dicho acceso deberá ser facilitado por la autoridad expedidora, o en su nombre» (Convenio Internacional del Trabajo núm. 185, párrafo 9 del artículo 3). «La plantilla biométrica [corresponderá] a una huella dactilar impresa en forma de números en un código de barras, acorde con una norma» [la presente norma] (Convenio Internacional del Trabajo núm. 185, anexo I).

La autoridad expedidora dará a los marinos acceso a las máquinas que les permitirán consultar los datos almacenados en el código de barras bidimensional PDF417 de su DIM. El marino podrá verificar si las plantillas de las huellas dactilares almacenadas en su tarjeta coinciden con las huellas registradas. Los datos que no sean relativos a las huellas dactilares se presentarán en forma de texto.

5.4.2. Base electrónica de datos nacional de los DIM

En el Convenio núm. 185 de la OIT se prevé una serie de requisitos que cada Miembro debe o debería cumplir en relación con la base electrónica de datos nacional de los DIM. Estos requisitos, que incidirán en la aplicación y la utilización del sistema de reconocimiento biométrico, se destacan a continuación junto con la estrategia de cumplimiento preconizado por las autoras del presente perfil biométrico.

- «Los datos que deberán suministrarse para cada asiento abierto en la base electrónica de datos que todos los Miembros habrán de mantener al día en virtud de los párrafos 1, 2, 6 y 7 del artículo 4 del presente Convenio [de la Conferencia Internacional del Trabajo] [núm. 185], serán exclusivamente los siguientes:

  1. Autoridad expedidora indicada en el documento de identidad.
  2. Nombre completo del marino, tal como conste en el documento de identidad.
  3. Número único del documento.
  4. Fecha de caducidad, suspensión o retiro del documento de identidad.
  5. Plantilla biométrica que figura en el documento de identidad.
  6. Fotografía (de estar almacenada en formato digital).
  7. Pormenores sobre toda solicitud de información acerca de los documentos de identidad de la gente de mar.» (Convenio Internacional del Trabajo núm. 185, anexo II).

En la base electrónica de datos nacional se registrarán los siete extremos antes enumerados para cada DIM expedido a un marino.

- «A los efectos del presente Convenio, se establecerán restricciones apropiadas a fin de que ningún dato, en particular las fotografías, pueda ser intercambiado, a menos que se instaure un mecanismo que garantice el cumplimiento de las normas aplicables en materia de protección de datos y de privacidad.» (Convenio Internacional del Trabajo núm. 185, artículo 4, párrafo 6.)

Se instaurarán mecanismos de control del acceso a la base de datos para proteger la información relativa a los marinos frente a las personas no autorizadas y a toda actuación desviada.

- «Los datos indicados en los puntos del anexo II [al Convenio Internacional del Trabajo núm. 185] se [introducirán] en la base de datos al tiempo que se expidan los DIM correspondientes.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte A, párrafo 3, apartado *b)* inciso i)).

Las bases electrónicas de datos de todos los Miembros se actualizarán oportunamente cada vez que se expida un nuevo DIM.

- «Todo Miembro velará por que se conserve en una base electrónica de datos constancia de cada documento de identidad de la gente de mar que haya sido expedido, suspendido o retirado. Deberán adoptarse las medidas necesarias para proteger esta base de datos frente a toda injerencia o acceso no autorizados.» (Convenio Internacional del Trabajo núm. 185, artículo 4, párrafo 1). «El documento de identidad de la gente de mar será retirado rápidamente por el Estado que lo haya expedido si se determinase que el marino titular ha dejado de reunir las condiciones requeridas en el presente Convenio.» (Convenio Internacional del Trabajo núm. 185, artículo 7, párrafo 2). «La autoridad expedidora debería instaurar procedimientos adecuados para proteger la base de datos, en particular permitir únicamente a los funcionarios especialmente habilitados tener acceso a las entradas de la base de datos o modificar estas últimas, una vez que hayan sido confirmadas por el funcionario responsable de ellas.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 4.2.2).

En las bases electrónicas de datos nacionales de los Miembros se incluirá una función de comprobación sobre las operaciones siguientes: la expedición de los DIM, su suspensión y su retiro. Se utilizarán mecanismos para controlar el acceso a la base de datos a fin de proteger la información relativa a los marinos frente a las personas no autorizadas y actuaciones desviadas. Los funcionarios especialmente autorizados de la entidad responsable en cada Estado Miembro deberían tener facultades limitadas para introducir cambios en el diario de comprobación. Los Miembros guardarán constancia de cada uno de estos cambios.

- «[Se adoptarán rápidamente] medidas para actualizar la base de datos cada vez que se suspenda o se retire un DIM.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte A, párrafo 3, apartado *c)*).

Las bases electrónicas de datos nacionales de cada Miembro se actualizarán oportunamente cada vez que se suspenda un DIM o que se retire.

- «[Se instaurará] un sistema de prórroga o de renovación para atender a las situaciones en que el marino necesite que se prorrogue o se renueve su DIM, o en que se le haya perdido el DIM.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte A, párrafo 3, apartado *d)*). «Mientras el solicitante sea titular de un DIM, no se le debería expedir otro DIM.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 3.9).

Los Miembros aplicarán un sistema de prórroga o de renovación para atender a las situaciones en que un marino necesite que se prorrogue o se renueve su DIM, o en que se le haya perdido este último. Esta prórroga o renovación se hará constar oportunamente en la base electrónica de datos nacional. De rechazarse un DIM en caso de caducidad, se consultará la base electrónica de datos a fin de averiguar si el DIM ha sido prorrogado o renovado. Los marinos no deberían tener más de un DIM a la vez. La reexpedición de un DIM debería invalidar todo DIM anteriormente expedido al marino de que se trate. El sistema de reconocimiento biométrico vendrá a facilitar el nuevo registro del DIM o su nueva expedición.

- «Debería aplicarse un sistema de renovación anticipado cuando un marino sepa de antemano, atendiendo al período en que deba prestar su servicio, que no estará en condiciones de presentar su solicitud de renovación cuando llegue la fecha de caducidad.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 3.9.1.) «Mientras el solicitante sea titular de un DIM, no se le debería expedir otro DIM.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 3.9).

Los Miembros instaurarán un sistema de prórroga y/o renovación para atender a las situaciones en que el marino necesite que se prorrogue o se renueve su DIM. El marino podrá solicitar, en su caso, una prórroga y/o una renovación, cuando no pueda presentar su solicitud de renovación en circunstancias normales. La prórroga y/o renovación de un DIM se hará constar oportunamente en la base electrónica de datos. De ser rechazado un DIM por causa de caducidad, se consultará la base de datos nacional a fin de verificar si el DIM ha sido prorrogado o renovado. Los marinos sólo deberían tener un DIM a la vez. La nueva expedición de un DIM debería invalidar todo DIM previamente expedido al marino. El sistema de reconocimiento biométrico vendrá a facilitar el nuevo registro del DIM o su nueva emisión.

- «Debería aplicarse un sistema de sustitución en caso de pérdida de un DIM. Cabría expedir un documento provisional apropiado.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 3.9.3.) «Mientras el solicitante sea titular de un DIM, no se le debería expedir otro DIM.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 3.9.)

Los Miembros instaurarán un sistema de sustitución para atender a las situaciones en que un marino haya perdido su DIM. La sustitución de un DIM se hará constar en tiempo real en la base electrónica de datos nacional. Los marinos sólo deberían tener un DIM a la vez. De expedirse nuevamente un DIM, el DIM previamente expedido al marino debería quedar invalidado. El sistema de reconocimiento biométrico vendrá a facilitar la nueva inscripción del DIM o su nueva expedición. El marino podrá instar, en su caso, un DIM de repuesto por cualquier documento provisional. Deberá devolverse el documento provisional. La base electrónica de datos nacional se actualizará oportunamente a fin de reflejar los cambios pertinentes. Sólo la autoridad expedidora del DIM original podrá expedir documentos provisionales.

- «La autoridad expedidora debería instaurar procedimientos adecuados para proteger la base de datos, en particular la obligación de realizar periódicamente copias de seguridad de la base de datos, las cuales se almacenarán en soportes informáticos conservados en un lugar seguro, fuera de los locales de la autoridad expedidora.» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 4.2.2.)

La autoridad expedidora de cada Miembro debería realizar periódicamente copias de seguridad de la base electrónica de datos que deberían almacenarse en soportes informáticos conservados en lugar seguro, fuera de los locales de la autoridad expedidora.

- La autoridad expedidora de cada Miembro debería llevar un registro de «los problemas advertidos en relación con la fiabilidad o seguridad de la base electrónica de datos, incluidas las solicitudes de información en la base de datos» (Convenio Internacional del Trabajo núm. 185, anexo III, parte B, párrafo 5.6.5.)

Las bases electrónicas de datos de los Miembros cumplirán una función de comprobación que permitirá tomar nota de los problemas que incidan en la fiabilidad o la seguridad de la base electrónica de datos (inclusive las solicitudes de información dirigidas a la base de datos).

Annex A

SID minutiae-based fingerprint bar code format (normative)

The SID PDF417 2-D bar code shall have 16 data symbol columns and 40 rows, utilizing error correction level 5. The data shall be recorded using byte mode. There shall be up to 686 bytes of data total in the SID minutiae-based fingerprint bar code format, described below. The data area shall be padded with enough pad codewords (value 900) to make exactly 40 even rows. The seafarers' fingerprint biometric data shall be recorded using the format specified in Annex B followed immediately thereafter by a set of metadata that is both printed on the surface of the SID in text and in the bar code to support seafarer authentication. The fields shall be defined as follows:

1. Fingerprint data.
   Data for two fingerprint templates in BioAPI compliant format shall be stored as specified in Annex B.

2. Issuing authority.
   The country code of the issuing authority shall be stored as an unsigned integer in two bytes.

3. Document number.
   A text stream of up to nine characters shall be stored in nine bytes. The stream consisting of the issuing authority and the document number shall be unique.

4. Personal identification number.
   An optional null terminated text stream of up to 14 characters shall be stored in 14 bytes. A stream of 14 null bytes may be stored instead.

5. Expiration date.
   The date of expiry shall be stored in SSE format.

6. Primary identification.
   The primary identification shall be stored using a null-terminated text stream in 20 bytes using up to 20 characters.

7. Secondary identification.
   The secondary identification shall be stored using a null-terminated text stream in 20 bytes using up to 20 characters.

8. Nationality.
   The country code representing the seafarer's nationality shall be stored as an unsigned integer in two bytes.

9. Place of birth.
   The place of birth shall be stored using a null-terminated text stream in 20 bytes using up to 20 characters.

10. Date of birth.
    The date of birth shall be stored in SSE format.

11. Gender.
    The gender of the seafarer shall be stored using a character "m" (0x6D) or "f" (0x66) or "x" (0x78).

12. Date of issue.
    The date of issue shall be stored in SSE format.

13. Place of issue.
    The place of issue shall be stored using a null-terminated text stream in 20 bytes.

Minutiae-based fingerprint SID bar code format (informative)

Field	Size	Comments
Fingerprint data	Up to 566 bytes	See Annex B
Issuing authority	2 bytes	Country code (see note 1)
Document number	9 bytes	Text (see note 1)
Personal identification number	14 bytes	Optional text
Expiry date	4 bytes	SSE
Primary identifier	20 bytes	Text
Secondary identifier	20 bytes	Text
Nationality	2 bytes	Country code
Place of birth	20 bytes	Text
Date of birth	4 bytes	SSE
Gender	1 byte	“m” (0x6D) or “f” (0x66) or “x” (0x78).
Date of issue	4 bytes	SSE
Place of issue	20 bytes	Text

Note 1: The issuing authority plus the document number comprise the unique document identifier.

Annex B

SID bar code minutiae-based fingerprint storage format (normative)

The SID bar code will be generated in a fixed format to support international interoperability. Data for two minutiae-based fingerprints will be stored in a fixed-size PDF417 bar code structure in accordance with ISO/IEC 15438:2001 that uses the draft ISO/IEC minutiae-based fingerprint interchange format (ISO/IEC CD 19794-2 (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003)) to encode two fingerprints with up to 52 minutiae each, and wrapped inside a BioAPI template as outlined in the table below.

Because this fingerprint storage format was developed in accordance with draft ISO standard documents, which are known to be in flux, *this document will take precedence for the seafarers' ID* should evolution of either of these draft standards create any perceived inconsistency. Copies of the two draft conformance standards; namely, ISO CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003) and ISO WD 19794-4 – Biometric data interchange formats – Part 4: Finger image-based interchange format (ISO/IEC JTC 1 SC37 N 341, dated 7 October 2003), are provided in Annex C and Annex D, respectively.

Many values will be the same for every template, as indicated below. Refer to Annex C for encoding details. Note that the finger minutiae normal card format, which does not include delta, core, ride count, or other extended data, has been chosen to support the seafarers' ID application. In no event shall an optional field be skipped. All fields marked as "Fixed" shall not contain values other than those present. Some fields are "RIU" – Reserved for implementers use. To assist in implementation, many field names from the BioAPI standard are used here.

The format is defined as follows, with an informative summary table at the end.

All values are stored without field delineators. Indexing is by byte-count. Hexadecimal notation is used unless otherwise noted.

1. The BioAPI header value shall be 16 bytes long and be 0x00000238010401010020 3nn0200000008 – where nn is the signed integer with the value of 1 through 100 corresponding to the overall quality of these fingerprints.
2. After the BioAPI header comes the opaque biometric data, in this case the finger minutiae-based template format as defined in Annex C (ISO/IEC CD 19794-2 (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003)).
3. At the start of the finger minutiae-based template is a header. The following values shall be fixed:
   (a) the "version number" field value shall be 0x20313100 corresponding to version 1.1;
   (b) the "length of record" field value shall be up to 0x0226 corresponding to up to 550 bytes (the "opaque biometric data", which encompasses 1st and 2nd fingerprint and finger minutiae data given in informative table below);
   (c) the "number of fingers in record" field value shall be 0x01 corresponding to the storage of two fingerprints;
   (d) the "number of finger views" field value shall be 0x00 corresponding to only one view per finger.
4. After the minutiae-based fingerprint template header are the two fingerprint templates themselves. A header prefixes each fingerprint template. The following values shall be fixed:
   (a) the "finger location" fields shall contain a value no less than 0x01 and no greater than 0x0A. The value shall correspond to the finger stored. See section 5.1.1 for finger order preference. The values are as follows: 0x01 = Right thumb; 0x02 = Right index finger; 0x03 = Right middle finger; 0x04 = Right ring finger; 0x05 = Right little finger; 0x06 = Left thumb; 0x07 = Left index finger; 0x08 = Left middle finger; 0x09 = Left ring finger; 0x0A = Left little finger;

(b) the "impression type" field value shall be either 0x00 (corresponding to a "Live-scan plain") or 0x08 (corresponding to "Swipe");

(c) the "view number" field value shall be 0x00 corresponding to one view;

(d) the finger minutiae data shall be stored in normal card format as specified in Annex C, section 8.1 – Normal size finger minutiae format.

5. All unspecified fields are governed by Annex C (ISO/IEC CD 19694-2 (dated 7 October 2003)).

SID minutiae-based fingerprint bar code storage format

Field	Size	Value	Comment
BioAPI_BIR (Biometric identification record)			
BioAPI_BIR_HEADER			
Length in bytes	4 bytes	Up to 0x00000236	Up to 566 bytes (length of record below + 16)
BioAPI_BIR_VERSION	1 byte	0x01	Fixed
BioAPI_BIR_DATA_TYPE	1 byte	0x04	Fixed – "Processed"
BioAPI_BIR_BIOMETRIC_DATA_FORMAT	4 bytes	0x01010203	Fixed – 0x0101 = JTC 1 SC37 format owner 0x0203 = Finger minutiae card format – normal size
BioAPI_Quality	1 byte		Signed integer
BioAPI_BIR_PURPOSE	1 byte	0x02	Fixed – value is equivalent to BioAPI_PURPOSE_IDENTIFY
BioAPI_BIR_AUTH_FACTORS	4 bytes	0x00000008	Fixed – value is equivalent to BioAPI_FACTOR_FINGERPRINT
BioAPI "Opaque biometric data"			
Format identifier	4 bytes	0x464D5200	Fixed – "FMR" 0x00
Version number	4 bytes	0x20313100	Fixed – "11" 0x00 [1]
Length of record	2 bytes	Up to 0x0226	Up to 550 bytes (total number of minutiae * 5 + 30)
Capture equipment compliance	4 bits		RIU
Capture equipment ID	12 bits		RIU
X (horizontal) image size	2 bytes		Pixels per centimetre
Y (vertical) image size	2 bytes		Pixels per centimetre
X (horizontal) resolution	2 bytes		Pixels per centimetre, not zero
Y (vertical) resolution	2 bytes		Pixels per centimetre, not zero
Number of fingers [2]	1 byte	0x01	Fixed – Two fingers
Number of finger views	1 byte	0x00	Fixed
1st fingerprint			
Finger position	1 byte	0x01 – 0x0A	0x02 = Right index finger 0x07 = Left index finger 0x01 = Right thumb 0x06 = Left thumb 0x03 = Right middle finger 0x08 = Left middle finger 0x04 = Right ring finger 0x09 = Left ring finger 0x05 = Right little finger

Field	Size	Value	Comment
			0x0A = Left little finger (From ANSI/NIST-ITL 1-2000, table 5)
View number	4 bits	0x0	Fixed
Impression type	4 bits	0x0 or 0x8	0x00 = Live-scan plain 0x08 = Swipe
Finger quality	1 byte	0x00-0x64	0-100
Number of minutiae	1 byte	Up to 0x34	Up to 52 minutiae [3]
Finger minutiae data	Up to 240 bytes		See Annex C.8.1
	2nd fingerprint		
Finger location	1 byte	0x01 – 0x0A	0x02 = Right index finger 0x07 = Left index finger 0x01 = Right thumb 0x06 = Left thumb 0x03 = Right middle finger 0x08 = Left middle finger 0x04 = Right ring finger 0x09 = Left ring finger 0x05 = Right little finger 0x0A = Left little finger (From ANSI/NIST-ITL 1-2000, table 5)
Impression type	1 byte	0x0 or 0x8	0x00 = Live-scan plain 0x08 = Swipe
Finger quality	1 byte	0x00-0x64	0-100
Number of minutiae	1 byte	Up to 0x34	Up to 52 minutiae [3]
Finger minutiae data	Up to 240 bytes		See Annex C.8.1

[1] To identify that this is the same format as ISO/IEC CD 19794-2. Note, the version number "1.1" indicates that there may be differences between this standard and the final international standard. [2] There is disagreement between specifying number of fingers or a reserved byte. [3] "If the number of minutiae exceeds the maximum number processable by a card, truncation is necessary. The truncation is a two-step process. At first, finger minutiae of poor quality are eliminated. If still too many minutiae are there, then truncation shall be made by peeling off minutiae from the convex hull of the minutiae set and before sorting into the order required by the card." (ISO/IEC CD 19794-2, dated 7 Oct. 2003 (ISO/IEC JTC 1 SC37 N 340, paragraph 8.3.1)).

Anexo C

ISO/IEC WD 19794-2 (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003)

ISO/IEC JTC 1/SC 37 N340

2003-10-07

Replaces:

ISO/IEC JTC 1/SC 37
Biometrics

Document Type: Text for CD ballot or comment

Document Title: Text of CD 19794-2, Biometric Data Interchange Formats — Part 2: Finger Minutiae Data

Document Source: Project Editor

Project Number:

Document Status: In accordance with Rome resolution 2.1, this document is circulated to SC 37 National Bodies for CD letter ballot.

Special Note: Recipients of this document are invited to submit notification of any relevant patent rights of which they are aware and to provide supporting documentation. This information should also be submitted to the SC 37 Secretariat by January 7, 2004.

Action ID: LB

Due Date: 2004-01-07

Distribution:

Medium:

Disk Serial No:

No. of Pages: 44

Secretariat, ISO/IEC JTC 1/SC 37, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC 19794-2	
Date: **2003-10-07**	Reference number: ISO/IEC JTC 1/SC 37 **N 340**
Supersedes document	

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 37 Biometrics Secretariat: USA (ANSI)	Circulated to P- and O-members, and to technical committees and organizations in liaison for: - discussion at - comment by **- voting by (P-members only)** **2004-01-07** Please return all votes and comments in electronic form directly to the SC 37 Secretariat by the due date indicated.

ISO/IEC JTC 1/SC 37

Title: Biometric Data Interchange Formats – Part 2: Finger Minutiae Data

Project: 1.37.19794.2

Introductory note:

As per Rome resolution 2.1, this document is circulated for CD letter ballot. Recipients of this document are invited to submit notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Address Reply to: Secretariat, ISO/IEC JTC 1/SC 37, Address: 25 West 43rd Street, New York, NY 10036
Telephone: +1-212-642-4932; Facsimile: +1 212-840-2298; E-Mail: LRAJCHEL@ANSI.org

ISO/IEC JTC 1/SC 37 N 340

Date: 2003-10-03

ISO/IEC CD 19794-2

ISO/IEC JTC 1/SC 37/WG 3

Secretariat: ANSI

Biometrics — Biometric Data Interchange Formats — Part 2: Finger Minutiae Data

Biométrie — Formats d'échanges de données biométriques — Partie 2: Dates des minuties du doigt

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (30) Committee
Document language: E

C:\Documents and Settings\lrajchel\Desktop\to do\ISO-IEC_19794-2_(E)_CD.doc STD Version 2.1

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19794-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 37.

ISO/IEC 19794 consists of the following parts, under the general title *Biometrics — Biometric Data Interchange Formats*:

— *Part 1: Framework*

— *Part 2: Finger Minutiae Data*

— *Part 3: Finger Pattern Data*

— *Part 4: Finger Image Data*

— *Part 5: Face Image Data*

— *Part 6: Iris Image Data*

— *Part 7: Signature/Sign Data*

Introduction

In the interest of implementing interoperable biometric recognition systems, this ISO/IEC Standard establishes a data interchange format for minutiae-based fingerprint capture and recognition equipment. Representation of fingerprint data using minutiae is a widely used technique in many application areas.

This Standard defines specifics of the extraction of key points (called *minutiae*) from fingerprint ridge patterns. Two types of data formats are then defined: one for general storage and transport, one for use in card-based systems; the card format has a standard and a compact expression.

The biometric data record specified in this standard shall be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB). The BDB_PID shall be defined by CBEFF.

The CBEFF BDB_biometric_organization assigned by the International Biometric Industry Association (IBIA) to JTC 1 SC 37 shall be used. This is the sixteen bit value 0x0101 (hexadecimal 101 or decimal 257). There are six different CBEFF BDB_format codes codes assigned to this standard, as described in Section 9.

Biometrics — Biometric Data Interchange Formats — Part 2: Finger Minutiae Data

1 Scope

This Standard specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. The standard is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. The Standard contains definitions of relevant terms, a description of where minutiae points shall be located, data formats for containing the data for both general use and for use with cards, and conformance information. Guidelines and values for matching and decision parameters are provided in an informative Annex.

2 Conformance

A system conforms to this standard if it satisfies the mandatory requirements herein for extraction of minutiae points from a fingerprint image as described in Section 6 and the generation of a minutiae data record as described in Section 7 (for general data interchange use) or Section 8 (for use with cards).

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, subsequent amendments to or revisions of any of these publications apply to this standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

ISO/IEC CD3 19785-1:2003 – Biometrics – Common Biometric Exchange Formats Framework (CBEFF) – Part 1: Data Element Specification

ISO/IEC WD 19785-2:2003 – Biometrics – Common Biometric Exchange Formats Framework (CBEFF) – Part 2: Procedures of the Operation of the Biometric Registration Authority

ISO/IEC FCD 19784:2003– *Information technology – BioAPI Specification*

ANSI/NIST-ITL 1-2000 – *Standard Data Format for the Interchange of Fingerprint, Facial & Scar. Mark & Tattoo (SMT) Information*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ?? and the following apply.

4.1
Algorithm
A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine (i.e., the biometric system software) to compute whether a biometric sample and template are a match.

4.2
Base Standard
Fundamental and generalized procedures. They provide an infrastructure that may be used by a variety of applications, each of which may make its own selection from the options offered by them.

4.3
Biometric
A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee.

4.4
Biometric Data
Data encoding a feature or features used in biometric verification.66400:2003 (E)

4.5
Biometric Sample
Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).

4.6
Biometric System
An automated system capable of:
1. capturing a biometric sample from an end user;
2. extracting biometric data from that sample;
3. comparing the biometric data with that contained in one or more reference templates;
4. deciding how well they match; and
5. indicating whether or not an identification or verification of identity has been achieved.

4.7
Capture
The method of taking a biometric sample from the end user.

4.8
Comparison
The process of comparing a biometric sample with a previously stored reference template or templates. See also ‘One-To-Many’ and ‘One-To-One’.

4.9
Claimant
A person submitting a biometric sample for verification or identification while claiming a legitimate or false identity.

4.10
Core
A core is the topmost point on the innermost recurving ridgeline of a fingerprint.

4.11
Database
Any storage of biometric templates and related end user information. Even if only one biometric template or record is stored, the database will simply be “a database of one”. Generally speaking, however, a database will contain a number of biometric records.

4.12
Delta
A Delta is that point on a ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence.

4.13
End User
[see User - different] A person who interacts with a biometric system to enroll or have his/her identity checked.

4.14
Enrollment
The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

4.15
Extraction
The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

4.16
Friction Ridge
The ridges present on the skin of the fingers and toes, the palms and soles of the feet, which makes contact with an incident surface under normal touch. On the fingers, the unique patterns formed by the friction ridges make up fingerprints.

4.17
Identification / Identify
The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with ‘Verification’.

4.18
Live Capture
The process of capturing a biometric sample by an interaction between an end user and a biometric system.

4.19
Live-Scan Print
A fingerprint image that is produced by scanning or imaging a live finger to generate an image of the friction ridges.

4.20
Match / Matching
The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

4.21
Minutia (single) Minutiae (pl)
Friction ridge characteristics that are used to individualize a fingerprint. Minutiae occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending, division, or a more complicated “composite” type.

4.22
Population
The set of end-users for the application.

4.23
Record
The template and other information about the end-user (e.g. access permissions).

4.24
Resolution
The number of pixels (picture elements) per unit distance in the image of the fingerprint.

4.25
Ridge Bifurcation
The minutiae point assigned to the location at which a friction ridge splits into two ridges or, alternatively, where two separate friction ridges combine into one.

4.26
Ridge Ending
The minutiae point assigned to the location at which a friction ridge terminates or, alternatively, begins. A ridge ending is defined as the bifurcation of the adjacent valley - the location at which a valley splits into two valleys or, alternatively, at which two separate valleys combine into one.

4.27
Ridge Skeleton Endpoint
The minutiae point assigned to the location at which a ridge skeleton ends. A ridge skeleton endpoint is defined as the ending of the skeleton of a ridge.

4.28
Skeleton
The single-pixel-wide representation of a ridge or valley obtained by successive symmetric thinning operations. The skeleton is also known as the medial axis.

4.29
Template / Reference Template
Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples. NOTE - this term is not restricted to mean only data used in any particular recognition method, such as template matching.

4.30
User
The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.

4.31
Valley
The area surrounding a friction ridge, which does not make contact with an incident surface under normal touch; the area of the finger between two friction ridges.

4.32
Valley Bifurcation
The point at which a valley splits into two valleys or, alternatively, where two separate valleys combine into one.

4.33
Verification / Verify
The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.

5 Symbols (and abbreviated terms)

The following abbreviations apply for the document:

BER	Basic Encoding Rules
BIT	Biometric Information Template
CBEFF	Common Biometric Exchange Formats Framework
DO	Data Object
FAR	False Acceptance Rate
FRR	False Rejection Rate
ICC	Integrated Circuit Card
RFU	Reserved for Future Use
TLV	Tag-Length-Value

6 Minutiae Extraction

This section defines the placement of minutiae on the fingerprint. Compatible minutiae extraction is required for interoperability between different finger matchers for the purposes of matching an individual against a previously collected and stored finger record. The interoperability is based on defining the finger minutiae extraction rules, record formats and card formats that are common to many finger matchers for acceptable matching accuracy, while allowing for extended data to be attached for use with equipment that is compatible with it.

6.1 Principle

Establishment of a common feature-based representation must rest on agreement on the fundamental notion for representing a fingerprint. Minutiae are points located at the places in the fingerprint image where friction ridges end or split into two ridges. Describing a fingerprint in terms of the location and direction of these ridge endings and bifurcations provides sufficient information to reliably determine whether two fingerprint records are from the same finger.

The specifications of minutia location and minutia direction described below accomplish this. See Figure 1 for an illustration of the definitions below.

6.2 Minutia Type

Each minutia point has a "type" associated with it. There are two major types of minutia: a "ridge ending" and a "ridge bifurcation" or split point. There are other types of "points of interest" in the friction ridges that occur much less frequently and are more difficult to define precisely. More complex types of minutiae are usually a

combination of the basic types defined above. This standard defines a category of “other” minutia for points that are not clearly a ridge ending or a bifurcation.

A ridge ending may — alternatively — be regarded as a valley bifurcation depending on the method to determine its position (see below). The format type of the biometric information template indicates the use of ridge endings or valley bifurcations.

6.3 Minutia Location

The minutia location is represented by its horizontal and vertical position. The minutiae determination strategy considered in this document relies on skeletons derived from a digital fingerprint image. The ridge skeleton is computed by thinning down the ridge area to single pixel wide lines. The valley skeleton is computed by thinning down the valley area to single pixel wide lines. If other methods are applied, they should approximate the skeleton method.

6.3.1 Coordinate System

The coordinate system used to express the minutia points of a fingerprint shall be a Cartesian coordinate system. Points shall be represented by their X and Y coordinates. The origin of the coordinate system shall be the upper left corner of the original image with X increasing to the right and Y increasing downward. Note that this is in agreement with most imaging and image processing use. When viewed on the finger, X increases from right to left as shown in Figure 1. All X and Y values are non-negative.

The X and Y coordinates of the minutia points shall be in pixel units, with the spatial resolution of a pixel given in the “X Resolution” and “Y Resolution” fields of the format. X and Y resolutions are stated separately.

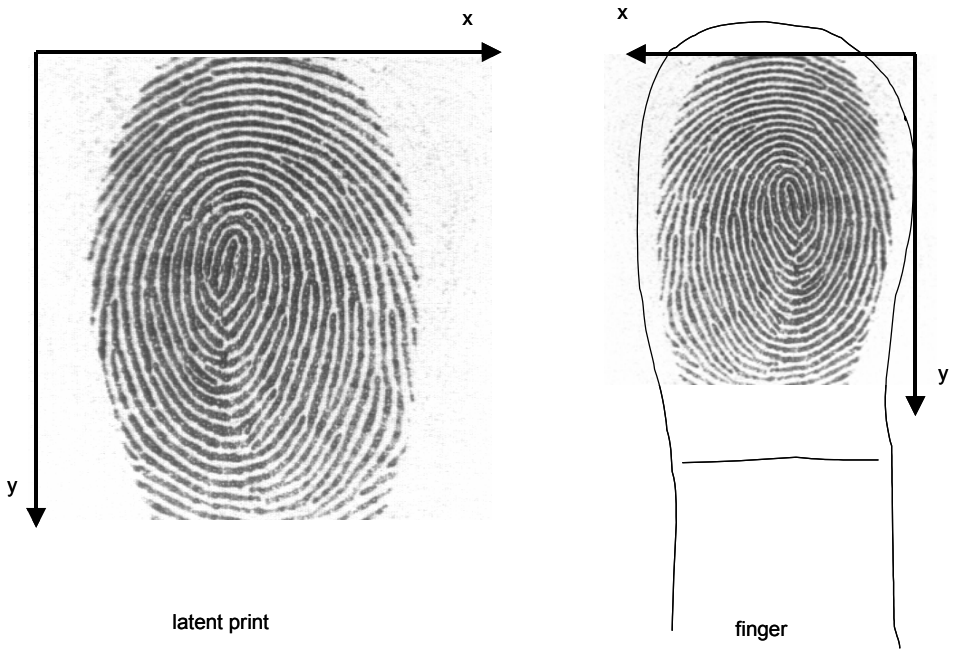


Figure 1 – Coordinate system

For the finger minutiae record format, the resolution of the coordinate system is specified in the record header, see 7.3.9 and 7.3.10. For the finger minutiae card format, the resolution of the X and Y coordinates of the minutia points shall be in metric units. The granularity is one bit per one hundredth of a millimeter in the normal format and one tenth of a millimeter in the compact format:

1 unit = 10^{-2} mm (normal format) or 10^{-1} mm (compact format).

6.3.2 Minutia Placement on a Ridge Ending (encoded as Valley Skeleton Bifurcation Point)

The minutia point for a ridge ending shall be defined as the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the valley area were thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia. In simpler terms, the point where the valley "Y"'s, or (equivalently) where the three legs of the thinned valley area intersect (see Fig. 2).

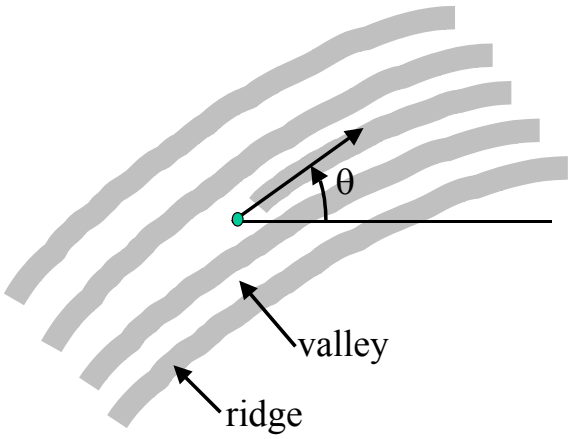


Figure 2 - Location and direction of a ridge ending (encoded as valley skeleton bifurcation point)

6.3.3 Minutiae Placement on a Ridge Bifurcation (encoded as a Ridge Skeleton Bifurcation Point)

The minutia point for a ridge bifurcation shall be defined as the point of forking of the medial skeleton of the ridge. If the ridge were thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia. In simpler terms, the point where the ridge "Y"'s, or (equivalently) where the three legs of the thinned ridge intersect (see Figure 3).

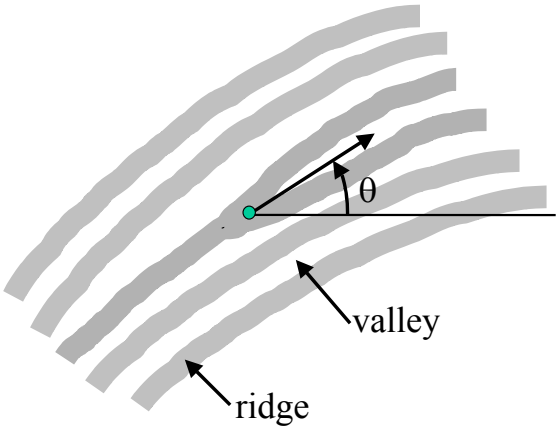


Figure 3 - Location and direction of a ridge bifurcation (encoded as ridge skeleton bifurcation point)

6.3.4 Minutiae Placement on a Ridge Skeleton Endpoint

The minutia point for a ridge skeleton endpoint shall be defined as the center point of the ending ridge. If the ridges in the digital fingerprint image were thinned down to a single-pixel-wide skeleton, the position of the minutia would be the coordinates of the skeleton point with only one neighbor pixel belonging to the skeleton (see Figure 4).

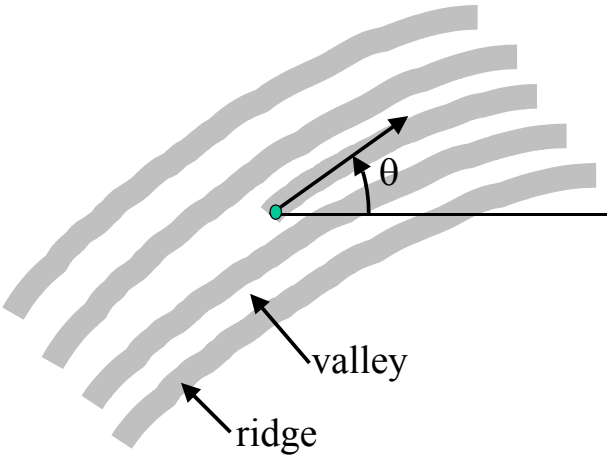


Figure 4 - Location and direction of a ridge skeleton endpoint

6.3.5 Minutiae Placement on Other Minutiae Types

For minutiae other than a bifurcation or ridge ending the placement and angle of direction shall be vendor defined.

6.3.6 Usage of the Minutiae Placement by the Record Formats and the Card Formats

The record formats use

- ridge ending and ridge bifurcation points.

The card formats use

- ridge ending and ridge bifurcation points, or

- valley skeleton bifurcation points and ridge bifurcation points

depending on the specific algorithms implemented. Typically, the card will request from a host system a minutiae record compatible with its matching algorithm. Both types of card formats are supported to avoid the on-card processing required to translate minutiae formats.

6.4 Minutia Direction

6.4.1 Angle Conventions

The minutiae angle is measured increasing counter-clockwise starting from the horizontal axis to the right.

In the record formats, the angle of a minutia is scaled to fit the granularity of 1.40625 (360/256) degrees per least significant bit.

The angle coding for the card formats depend on the normal size and the compact size format, see clause 8.1 and 8.2.

6.4.2 Minutia Direction of a Ridge Ending (encoded as Valley Skeleton Bifurcation Point)

A ridge ending (encoded as valley skeleton bifurcation point) has three arms of valleys meeting in one point. Two valleys encompass an acute angle. The tangent to the third valley lying opposite of the enclosed ridge defines the direction of a valley bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right (see Figure 2).

6.4.3 Minutia Direction of a Ridge Bifurcation (encoded as Ridge Skeleton Bifurcation Point)

A ridge bifurcation (encoded as ridge skeleton bifurcation point) has three arms of ridges meeting in one point. Two ridges encompass an acute angle. The tangent to the third ridge lying opposite of the enclosed valley defines the direction of a ridge bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right (see Figure 3).

6.4.4 Minutia Direction of a Ridge Skeleton End Point

The direction of a ridge skeleton endpoint is defined as the angle that the tangent to the ending ridge encompasses with the horizontal axis to the right (see Figure 4). Ridge skeleton end points are only used in

one type of the card formats, whereas in the other type ridge ending and ridge birfurcation is used as in the record format.

7 Finger Minutiae Record Format

7.1 Introduction

The minutiae record format shall be used to achieve interoperability between finger matchers providing a one-to-one verification. The minutia data shall be represented in a common format, containing both basic and extended data. With the exception of the Format Identifier and the Version number for the standard, which are null-terminated ASCII character strings, all data is represented in binary format. There are no record separators or field tags; fields are parsed by byte count.

7.2 Record Organization

The organization of the record is as follows:

- A fixed-length (24-byte) record header containing information about the overall record, including the number of fingers represented and the overall record length in bytes;
- A Single Finger record for each finger, consisting of:
- A fixed-length (4-byte) header containing information about the data for a single finger, including the number of minutiae;
- A series of fixed-length(6-byte) minutia point descriptions, including the position, type, angle and quality of the minutia point;
- One or more “extended” data areas for each finger, containing optional or vendor-specific information.

All multibyte quantities are represented in Big-Endian format; that is, the more significant bytes of any multibyte quantity are stored at lower addresses in memory than (and are transmitted before) less significant bytes. All numeric values are fixed-length integer quantities, and are unsigned quantities.

7.3 Record Header

There shall be one and only one record header for the minutiae record, to hold information describing the identity and characteristics of device that generated the minutiae data

7.3.1 Format Identifier

The Finger Minutiae Record shall begin with the three ASCII characters “FMR”. followed by a zero byte as a NULL string terminator.

7.3.2 Version Number

The version number for the version of this standard used in constructing the minutiae record shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major revision number and the third character will represent the minor revision number.

Upon approval of this specification, the version number shall be " 20" (an ASCII space followed by an ASCII '2' and an ASCII '0').

7.3.3 Length of Record

The length of the entire record shall be recorded in four bytes.

7.3.4 Capture Equipment Certifications

This field contains four bits used to indicate that the capture equipment used to capture the original fingerprint image was compliant with a standard certification method for such equipment. Currently, only the most significant bit is defined; if this bit is '1', the original capture equipment was certified to be compliant with the US Federal Bureau of Investigation's Image Quality Specifications, Appendix F. Three additional bits are reserved for future image quality certifications.

7.3.5 Capture Device ID

The capture device ID shall be recorded in twelve bits. A value of all zeros will be acceptable and will indicate that the capture device ID is unreported. The vendor determines the value for this field. Applications developers may obtain the values for these codes from the vendor.

7.3.6 Size of Scanned Image in X direction

The size of the original image in pixels in the X direction shall be contained in two bytes.

7.3.7 Size of Scanned Image in Y direction

The size of the original image in pixels in the Y direction shall be contained in two bytes.

7.3.8 X (horizontal) resolution

The resolution of the minutiae coordinate system shall be recorded in two bytes having the units of pixels per centimeter. The value of the sensor X resolution shall not be zero.

7.3.9 Y (vertical) resolution

The resolution of the minutiae coordinate system shall be recorded in two bytes having the units of pixels per centimeter. The value of the sensor Y resolution shall not be zero.

7.3.10 Number Of Fingers

The number of fingers contained in the minutiae record shall be recorded in one byte.

7.3.11 View Number

If more than one finger minutiae record in a general record is from the same finger, each minutiae record shall have a unique view number. The combination of finger location and view number shall uniquely identify a particular minutiae record within a general record. Multiple finger minutiae records from the same finger shall be numbered with increasing view numbers, beginning with zero. Where only one finger minutiae record is taken from each finger, this field shall be set to 0.

7.4 Single Finger Record Format

7.4.1 Finger Header

A finger header shall start each section of finger data providing information for that finger. There shall be one finger header for each finger contained in the finger minutiae record. The finger header will occupy a total of four bytes as described below. Note that it is permissible for more than one finger record to represent the same finger, with (presumably) different data, perhaps in the private area.

7.4.1.1 Finger Position

The finger position shall be recorded in one byte. The codes for this byte shall be as defined in Table 5 of ANSI/NIST-ITL 1-2000, “Data Format for the Interchange of Fingerprint Information”. This table is reproduced here in Table 1 for convenience. Only codes 0 through 10 shall be used; the “plain” codes are not relevant for this standard.

Table 1 - Finger Position Codes

Finger position	Code
Unknown finger	0
Right thumb	1
Right index finger	2
Right middle finger	3
Right ring finger	4
Right little finger	5
Left thumb	6
Left index finger	7
Left middle finger	8
Left ring finger	9
Left little finger	10
Plain right thumb	*11*
Plain left thumb	*12*
Plain right four fingers	*13*
Plain left four fingers	*14*

7.4.1.2 Impression Type

The impression type of the finger images that the minutiae data was derived from shall be recorded in one byte. The codes for this byte are shown in Table 2. These codes are compatible with Table 4 of ANSI/NIST-ITL 1-2000, “Data Format for the Interchange of Fingerprint Information”, with the addition of the “swipe” type. The “swipe” type identifies data records derived from image streams generated by sliding the finger across a small sensor. Only codes 0 through 3 and 8 shall be used; the “latent” codes are not relevant for this standard.

Table 2 - Impression Type Codes

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3

Latent impression	*4*
Latent tracing	*5*
Latent photo	*6*
Latent lift	*7*
Swipe	8

7.4.1.3 Finger Quality

The quality of the overall finger minutiae data shall be between 0 and 100 and recorded in one byte. This quality number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutia record. A value of 0 shall represent the lowest possible quality and the value 100 shall represent the higher possible quality. The numeric values in this field will be set in accordance with the general guidelines contained in Section 2.1.42 of ANSI/INCITS 358-2002, "BioAPI H-Level Specification Version 1.1". The matcher may use this value to determine its certainty of verification.

7.4.1.4 Number of Minutiae

The number of minutiae recorded for the finger shall be recorded in one byte.

7.4.2 Finger Minutiae Data

The finger minutiae data for a single finger shall be recorded in blocks of six bytes per minutia point. The order of the minutiae is not specified.

7.4.2.1 Minutiae Type

The type of minutiae will be recorded in the first two bits of the upper byte of the X coordinate. There will be two bits reserved at the beginning of the upper byte of the Y coordinate for future use. The bits "00" will represent a minutia of "other" type, "01" will represent a ridge ending and "10" will represent a bifurcation.

7.4.2.2 Minutiae Position

The X coordinate of the minutia shall be recorded in the rest of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header. Note that position information shall be present for each minutia point, regardless of type, although position for minutiae of type "other" is vendor defined.

7.4.2.3 Minutiae Angle

The angle of the minutia shall be recorded in one byte in units of 1.40625 (360/256) degrees. The value shall be a non-negative value between 0 and 255, inclusive. For example, an angle value of 16 represents 22.5 degrees. Note that angle information shall be present for each minutia point, regardless of type, although angle for minutiae of type "other" is vendor defined.

7.4.2.4 Minutiae Quality

The quality of each minutia shall be recorded in one byte. The quality figure shall range from 100 as a maximum to 1 as a minimum. In interoperable use, only the relative values of minutiae quality values is meaningful; there is no guaranteed relationship between minutiae quality values assigned by different equipment suppliers. Any equipment that does not supply quality information for individual minutia points shall set all quality values to 0.

7.5 Extended Data

The extended data section of the finger minutiae record is open to placing additional data that may be used by the matching equipment. The size of this section shall be kept as small as possible, augmenting the data stored in the standard minutiae section. The extended data for each finger shall immediately follow the standard minutiae data. More than one extended data area may be present for each finger. In this case, the length of data fields may be used to index through the fields, relative to the overall length of record field in the record header.

While the extended data area allows for inclusion of proprietary data within the minutiae format, this is not intended to allow for alternate representations of data that can be represented in open manner as defined in this standard. In particular, ridge count data and core and delta information shall not be represented in proprietary manner to the exclusion of the publicly defined formats in this standard. Additional ridge count or core and delta information may be placed in a proprietary extended data area if the standard fields defined below are also populated. The intention of this standard is to provide interoperability.

7.5.1 Common Extended Data Fields

All records shall contain at least the type identification code (Section 7.5.1.1). If this code is all zeroes (0x0000 hexadecimal), then there is no extended data and the length of data and data areas (Sections 7.5.1.2 and 6.5.1.3) shall not be present.

7.5.1.1 Type Identification Code

The type identification code shall be recorded in two bytes, and shall distinguish the format of the extended data area (as defined by the Vendor specified by the PID code in the CBEFF header). A value of zero in both bytes shall indicate that there is no following extended data. A value of zero in the first byte, followed by a non-zero value in the second byte, shall indicate that the extended data section has a format defined in this standard. A non-zero value in the first byte shall indicate a vendor specified format, with a code maintained by the vendor. Refer to Table 3 for a summary of the type identification codes.

Table 3 - Extended Data Area Type Codes

First byte	Second byte	Identification
0x00	0x00	no extended data
0x00	0x01	ridge count data (Section 7.5.2)
0x00	0x02	core and delta data (Section 7.5.3)
0x00	0x03	zonal quality data (Section 7.5.4)
0x00	0x04-0xFF	reserved
0x01-0xFF	0x00	reserved
0x01-0xFF	0x01-0xFF	vendor-defined extended data

7.5.1.2 Length of Data

The length of the extended data section, including the vendor identification and length of data fields, shall be recorded in two bytes. This value is used to skip to the next finger minutiae data if the matcher cannot decode and use this data. If the type identification (field 7.5.1.1) for the private area is zero, indicating no private data, this field shall not be present.

7.5.1.3 Data Section

The data field of the extended data is defined by the equipment that is generating the finger minutiae record, or by common extended data formats contained in this standard; see section 6.5.2. If the type identification (field 7.5.1.1) for the private area is zero, indicating no private data, this field shall not be present.

7.5.2 Ridge Count Data Format

If the extended data area type code is 0x0001, the extended data area contains ridge count information. This format is provided to contain optional information about the number of fingerprint ridges between pairs of minutiae points. Each ridge count is associated with a pair of minutiae points contained in the minutiae data area defined in section 6.4.2; no ridge information may be contained that is associated with minutiae not included in the corresponding minutiae area. Ridge counts shall not include the ridges represented by either of the associated minutiae points. Refer to Figure 5 for clarification; the ridge count between minutiae A and B is 1, while the ridge count between minutiae B and C is 2.

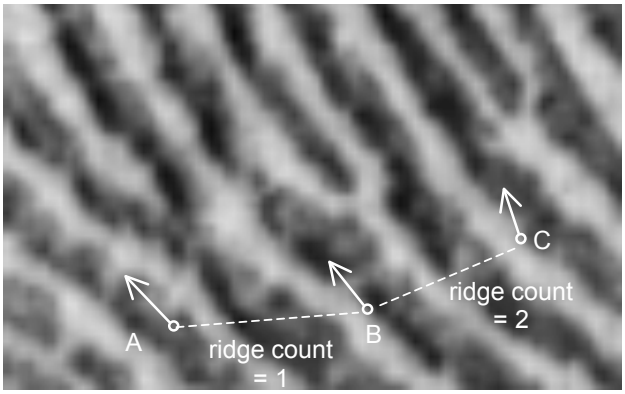


Figure 5 - Example Ridge Count data

7.5.2.1 Ridge Count Extraction Method

The ridge count data area shall begin with a single byte indicating the ridge count extraction method. Ridge counts associated with a particular center minutiae point are frequently extracted in one of two ways: by extracting the ridge count to the nearest neighboring minutiae in each of four angular regions (or quadrants), or by extracting the ridge count to the nearest neighboring minutiae in each of eight angular regions (or octants). The ridge count extraction method field shall indicate the extraction method used, as shown in Table 4.

Table 4 - Ridge Count Extraction Method Codes

RCE method field value	Extraction method	Comments
0x00	Non-specific	No assumption shall be made about the method used to extract ridge counts, nor their order in the record; in particular, the counts may not be between nearest-neighbor minutiae
0x01	Four-neighbor	For each center minutiae used, ridge count data was extracted to the nearest neighboring minutiae in four

	(quadrants)	quadrants, and ridge counts for each center minutiae are listed together
0x02	Eight-neighbor (octants)	For each center minutiae used, ridge count data was extracted to the nearest neighboring minutiae in eight octants, and ridge counts for each center minutiae are listed together

If either of these specific extraction methods are used, the ridge counts shall be listed in the following way:

- all ridge counts for a particular center minutiae point shall be listed together;
- the center minutiae point shall be the first minutiae point references in the three-byte ridge count data;
- if a given quadrant or octant has no neighboring minutiae in it, a ridge count field shall be recorded with both the minutiae index and the ridge count fields set to zero (so that, for each center minutiae, there shall always be four ridge counts recorded for the quadrant method and eight ridge counts recorded for the octant method);
- no assumption shall be made regarding the order of the neighboring minutiae.

Example - (Informative) If the extraction method code is 0x01, and ridge counts were extracted for minutiae numbers 5 and 22, the four ridge counts for minutiae number 22 could be listed first, followed by all four ridge counts for minutiae number 5.

7.5.2.2 Ridge Count Data

The ridge count data shall be represented by a list of three-byte elements. The first and second bytes are an index number, indicating which minutiae points in the corresponding minutiae area are being considered. The third byte is a count of the ridges intersected by a direct line between these two minutiae points.

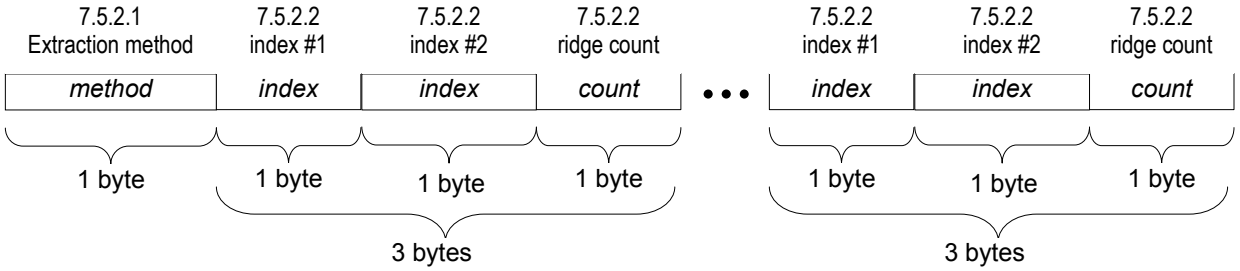
The ridge count data shall be listed in increasing order of the index numbers, as shown in Table 5. There is no requirement that the ridge counts be listed with the lowest index number first. Since the minutiae points are not listed in any specified geometric order, no assumption shall be made about the geometric relationships of the various ridge count items.

Table 5 - Example Ridge Count Data

Minutiae index #1	Minutiae index #2	Ridge count
0x01	0x02	0x05
0x01	0x06	0x09
0x01	0x07	0x02
0x02	0x04	0x13
0x02	0x09	0x0D
0x05	0x03	0x03
0x09	0x15	0x08

7.5.2.3 Ridge Count Format Summary

The ridge count data format shall be as follows:



7.5.3 Core and Delta Data Format

If the extended data area type code is 0x0002, the extended data area contains core and delta information. This format is provided to contain optional information about the placement and characteristics of the cores and deltas on the original fingerprint image. Core and delta points are determined by the overall pattern of ridges in the fingerprint. There may be one or more core points and zero or more delta points for any fingerprint. Core and delta points may or may not include angular information.

The core and delta information shall be represented as follows. The first byte shall contain the core information type and the number of core points included; legal values are 1 or greater. This length byte shall be followed by the position and angular information for the cores. The next byte shall contain the delta information type and the number of delta points included; legal values are 0 or greater. This length byte shall be followed by the position and angular information for the deltas.

7.5.3.1 Core Information Type

The core information type shall be recorded in the first two bits of the upper byte of the number of cores. The bits “00” will indicate that the core has angular information while “01” will indicate that no angular information is relevant for the core type. If this field is “00”, then the angle fields shall not be present for the cores.

7.5.3.2 Number of Cores

The number of core points represented shall be recorded in the least significant four bits of this byte. Valid values are from 0 to 15.

7.5.3.3 Core Position

The X coordinate of the core shall be recorded in the lower fourteen bits of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header.

7.5.3.4 Core Angle

The angle of the core shall be recorded in one byte in units of 1.40625 (360/256) degrees. The value shall be a non-negative value between 0 and 255, inclusive. For example, an angle value of 16 represents 22.5 degrees. If the core information type is zero (see Section 6.5.3.1), then this field shall not be present.

7.5.3.5 Delta Information Type

The delta information type shall be recorded in the first two bits of the upper byte of the number of deltas. The bits “00” will indicate that the delta has angular information while “01” will indicate that no angular information is relevant for the delta type. If this field is “00”, then the angle fields shall not be present for the deltas.

7.5.3.6 Number of Deltas

The number of delta points represented shall be recorded in the least significant four bits of this byte. Valid values are from 0 to 15.

7.5.3.7 Delta Position

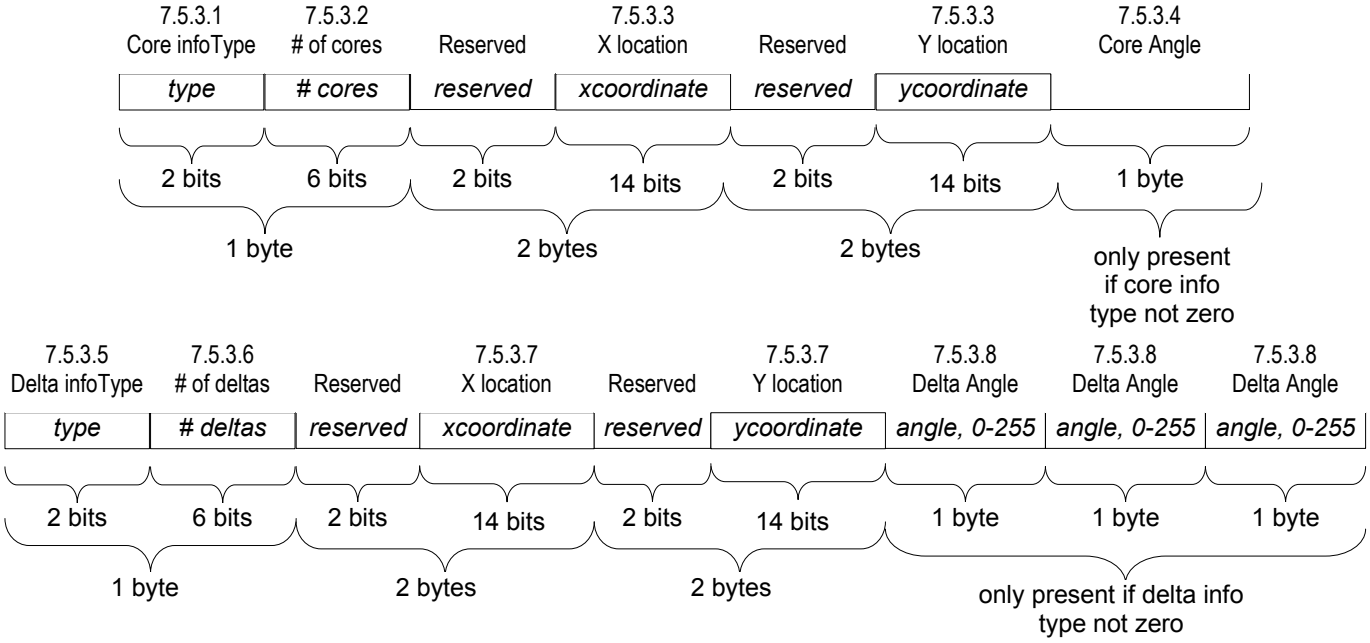
The X coordinate of the delta shall be recorded in the lower fourteen bits of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header.

7.5.3.8 Delta Angles

The three angle attributes of the delta shall be recorded in one byte in units of 1.40625 (360/256) degrees. The value shall be a non-negative value between 0 and 255, inclusive. For example, an angle value of 16 represents 22.5 degrees. If the delta information type is zero (see Section 7.5.3.5), then this field shall not be present.

7.5.3.9 Core and Delta Format Summary

The core and delta format shall be as follows:



7.5.4 Zonal Quality Data

If the extended data area type code is 0x0003, the extended data area contains zonal quality data. This format is provided to contain optional information about the quality of the fingerprint image within each cell in a grid defined on the original fingerprint image. Within each cell, the quality may depend on the presence and clarity of ridges, spatial distortions and other characteristics.

The zonal quality data shall be represented as follows. The first two bytes shall contain the horizontal and vertical cell sizes in pixels. These size bytes shall be followed by the quality indications for each cell, with one bit for each cell. The cell quality bits shall be packed into bytes, padded with zeroes on the right to complete the final byte. All cells are the same size, with the exception of the final cells in each row and in each column. The final cell in each row and in each column may be less than the stated cell size, if the cell width and height are not factors of the image width and height respectively.

7.5.4.1 Cell Width and Height

The number of pixels in cells in the x-direction (horizontal) shall be stored in one byte. Permissible values are 1 to 255.

The number of pixels in cells in the y-direction (vertical) shall be stored in one byte. Permissible values are 1 to 255.

7.5.4.2 Cell Data Length

The number of bytes containing the cell quality data shall be recorded in two bytes. The contents of this field shall be equal to the pixel width in the original image divided by the cell width, rounded up, multiplied by the pixel height of the original image divided by the cell height, rounded up, then divided by eight and rounded up.

$$CellDataLength(7.5.4.2) = ceil\left(\frac{ceil\left(\frac{XSizeofScannedImage\{7.3.7\}}{CellWidth\{7.5.4.1a\}} \right) ceil\left(\frac{YSizeofScannedImage\{7.3.8\}}{CellHeight\{7.5.4.1b\}} \right)}{8} \right)$$

where the function ceil() indicates the smallest integer greater or equal to the inner quantity. This field is included for convenience in reading the data record.

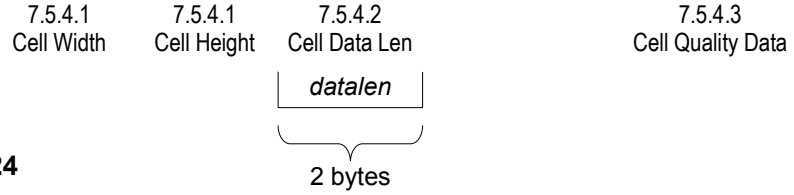
7.5.4.3 Cell Quality Data

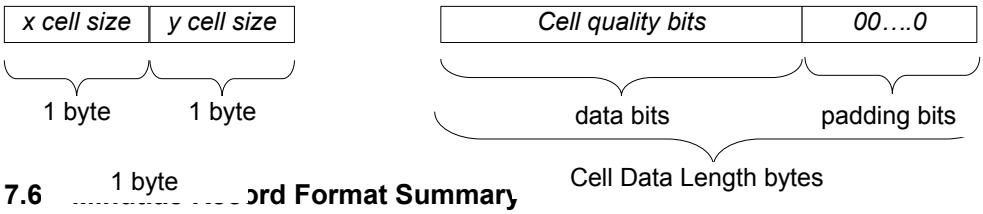
The quality of the fingerprint image in each cell shall be represented by one bit. If the finger image within this cell is of good clarity and significant ridge data is present, the cell quality shall be represented by the bit value '1'. If the cell does not contain significant ridge data, or the ridge pattern within the cell is blurred, broken or otherwise of poor quality, the cell quality shall be represented by the bit value '0'.

The cell quality shall be packed into bytes. The final byte in the cell quality data may be packed with bit values of zero ('0') on the right as required to complete the last byte.

7.5.4.4 Zonal Quality Data Format Summary

The zonal quality data format shall be as follows:





1 byte

7.6 ord Format Summary

Table 6 is a reference for the fields present in the Finger Minutia Record format. Optional extended data formats for ridge counts and core and delta information are not represented here. For more specific information, please refer to the text and to the Record Format Diagrams in Annex A.

Table 6 - Minutiae Record Format Summary

		Field	Size	Valid Values	Notes
One per record		Format Identifier	4 bytes	0x464D5200 ('F' 'M' 'R' 0x0)	"FMR " – finger minutiae record
		Version of this standard	4 bytes	n n n 0x0	" XX"
		Length of total record in bytes	4 bytes	26 – 65535, or 65536 - 4294967295	either 0x001A to 0xFFFF, or 0x000000010000 to 0x0000FFFFFFFF
		Capture Equipment Certification	4 bits		
		Capture Equipment ID	12 bits		Vendor specified
		Image Size in X	2 bytes		in pixels
		Image Size in Y	2 bytes		in pixels
		X (horizontal) Resolution	2 bytes		in pixels per cm
		Y (vertical) Resolution	2 bytes		in pixels per cm
		Number of Finger Views	1 byte	0 to 255	
		Reserved byte	1 byte	00	0 for this version of the standard
One per finger view		Finger Position	1 byte	0 to 11	Refer to ANSI/NIST standard
		View Number	4 bits	0 to 15	
		Impression Type	4 bits	0 to 3 or 8	
		Finger Quality	1 byte	0 to 100	0 to 100
		Number of Minutiae	1 byte		
One per minutia		X (minutia type in upper 2 bits)	2 byte		Expressed in image pixels
		Y (upper 2 bits reserved)	2 byte		Expressed in image pixels
		θ	1 byte	0 to 255	Resolution is 1.40625 degrees
		Quality	1 byte	0 to 100	1 to 100 (0 indicates "quality not reported")
One per view		Extended Data Block Length	2 bytes		0x0000 = no private area
Zero or more per view		Type Code for Extended Area	2 bytes		only present if Extended Data Block Length ≠ 0
		Length of extended data area	2 bytes		only present if Extended Data Block Length ≠ 0
		Extended data area	In prev. field		only present if Extended Data Block Length ≠ 0
		Each extended data area may contain vendor-specific data, or one of the following:			
Zero or more per view	Ridge count data	Ridge count extraction method	1 byte	0 to 2	
		Ridge count data – idx #1	1 byte	1 to # of minutiae	
		Ridge count data – idx #2	1 byte	1 to # of minutiae	
		Ridge count data – count	1 byte		
		additional ridge counts…			
Zero or more per view (may precede ridge count block)	Core and delta data	Core information type	2 bits	0 to 1	
		Number of cores	4 bits	0 to 15	
		X location	2 bytes		
		Y location	2 bytes		
		Angle (*if core info type ≠ 0)*	1 byte	0 to 255	
		Delta information type	2 bits	0 to 1	
		Number of deltas	4 bits	0 to 15	
		X location	2 bytes		
		Y location	2 bytes		
		Angles (*if delta info type ≠ 0)*	3 bytes	0 to 255	
	Zone quality	Cell Width	1 byte	1 to 255	
		Cell Height	1 byte	1 to 255	
		Cell Data Length	2 bytes	1 to 65536	
		Cell Quality Data	CellDataLen		

8 Finger Minutiae Card Format

This standard defines two card related encoding formats for finger minutiae, the normal size format and the compact size format. Such a format may be used e.g. as part of a Biometric Information Template as specified in ISO/IEC 7816-11 with incorporated CBEFF data objects, if off-card matching is applied, or in the command data field of a VERIFY command, if match-on-card (MOC) is applied (see ISO/IEC 7816-4 and -11).

NOTE – The term “card” is used for smartcards as well as for other kind of tokens.

8.1 Normal Size Finger Minutiae Format

With the normal size format, a minutia is encoded in 5 bytes (see Table 12):

- minutia type t (2 bits):
  00 = other,
  01 = ridge ending (encoded as valley skeleton bifurcation point), or ridge skeleton end point
  10 = ridge bifurcation (encoded as ridge skeleton bifurcation point)
  11 = reserved for future use

- coordinate x (14 bits), unit = 10^{-2} mm

- reserved (2 bits), default value: 00

- coordinate y (14 bits), unit = 10^{-2} mm

- angle θ (8 bits), unit = $2\pi/256$

Table 12 — Normal size finger minutiae format

type t	x-coordinate	reserved	y-coordinate	angle θ
2 bytes		2 bytes		1 byte

8.2 Compact Size Finger Minutiae Format

With the compact size format, only 3 bytes are used per minutia (see Table 13). This reduction of memory space is only possible at the cost of a reduction in resolution of coordinates and angle.

- coordinate x (8 bits), unit = 10^{-1} mm
- coordinate y (8 bits), unit = 10^{-1} mm
- minutia type t (2 bits): same coding as with the normal size format

- angle θ (6 bits), unit = $2\pi/64$

Table 13 — Compact size finger minutiae format

x-coordinate	y-coordinate	type t	angle θ
1 byte	1 byte	1 byte	

NOTE - The maximum value for the x and y coordinate is 25.5mm with the compact format.

8.3 Number of Minutiae, Minutiae Ordering Sequence and Truncation

8.3.1 General Aspects

The minutiae data of a finger consist of n minutia encoding shown in Table 12 (or alternatively Table 13). The number n depends on

- the minimum number of minutiae required according to the security level (see Annex C)
- the maximum number of minutiae accepted by a specific card e.g. due to buffer restrictions and computing capabilities.

The maximum number of minutiae accepted is therefore an implementation dependent value and shall be indicated in the Biometric Information Template, if the default value is not used (see Annex C).

A card may also require a special ordering of the minutiae presented in the biometric verification data. The ordering scheme shall be indicated in the Biometric Information Template (see ISO/IEC 19785 and ISO/IEC 7816-11), if the default value is not used.

If the number of minutiae exceeds the maximum number processible by a card, truncation is necessary. The truncation is a 2 step process. At first, finger minutiae of poor quality are eliminated. If still too many minutiae are there, then truncation shall be made by peeling off minutiae from the convex hull of the minutiae set and before sorting into the order required by the card.

8.3.2 Biometric matching algorithm parameters

Biometric matching algorithm parameters are used to indicate implementation specific values to be observed by the outside world when computing and structuring the biometric verification data. They can be encoded as DOs embedded in a biometric matching parameter template as defined in ISO/IEC 19785 (CBEFF Annex D, Table D.1).

8.3.3 Number of Minutiae

For the indication of the minimum and maximum value of minutiae expected by the card the DO Number of minutiae as shown in Table 14 shall be used.

Table 14 – Data Object for Number of Minutiae

Tag	L	Value
´81´	2	min (1 byte, binary coding) || max (1 byte, binary coding)

If this DO is not present in the BIT, the default values apply (see Annex C).

8.3.4 Minutiae Order

For the indication of the ordering scheme for minutiae, the DO Minutiae order as shown in Table 15 shall be used.

Table 15 – Data Object for Minutiae Order

Tag	L	Value
´82´	1	see Table 16

Table 16 – Values for Minutiae Order Indication

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	no ordering required (default value)
						0	1	ordered ascending
						1	0	ordered descending
			0	0	1			Cartesian x-y, see note 1
			0	1	0			Cartesian y-x
			0	1	1			Angle, see note 2
			1	0	0			Polar, root = center of mass
x	x	x						000, other values are RFU

NOTES –

1. Ordered by ascending/descending x-coordinate, if equal by ascending/descending y-coordinate (first x, then y)
2. The angle represents the orientation of the minutia.

The following description defines the ordering procedure in detail to avoid misunderstandings or misinterpretations.

Ordered ascending

Ordered ascending means, that the ordered sequence begins with the minutia from the original minutiae set, that has the smallest value of the indicated item. The value of this item increases with every successive minutia to the maximum value in the last minutia of the ordered sequence.

Ordered descending

Ordered descending means, that the ordered sequence begins with the minutia from the original minutiae set, that has the largest value of the indicated item. The value of this item decreases with every successive minutia to the minimum value in the last minutia of the ordered sequence.

Cartesian x-y

Cartesian x-y stands for an ordering scheme, where first the x-coordinate is compared and used for ordering. When ordering by ascending Cartesian x-y coordinates, the minutia with minimum x-coordinate becomes the first minutia in the ordered sequence. The minutia with the second smallest x-coordinate becomes the second minutia in the ordered sequence. This process continues until the minutia with maximum x-value becomes the last minutia in the ordered sequence. If the x-coordinates in two or more minutiae are equal, the y-coordinate is compared for ordering.

Cartesian y-x

Cartesian y-x stand for an ordering scheme, where first the y-coordinate is compared and used for ordering. If the y-coordinates in two or more minutiae are equal, the y-coordinate is compared for ordering.

Angle

Sorting a minutiae list by angle is done as follows. As defined in a previous section the angle of a minutia begins with value 0 to the right horizontal axis and increases counter-clockwise. When ordering by increasing angle, the minutia with the minimum angle value in the ordered sequence becomes the first minutia in the ordered sequence. The minutia with the second smallest angle value becomes the second minutia in the ordered sequence. This process continues until the last minutia in the ordered sequence is defined as the minutia with maximum angle value. No rules for subordering are defined, if the angle values in two or more minutiae are equal. Any possible ordering sequence of the minutiae with the same angle value is legal in this case.

Polar

Polar is an ordering sequence by ascending or descending polar coordinates. First of all, a virtual coordinate root is defined as the center of mass of all minutiae. The polar coordinates of every minutiae are computed as the relative distance and angle to this root coordinate. Without loss of generality, the process of ascending ordering with polar coordinates is described. The minutia with minimum distance to the root becomes the first minutia in the ordered sequence. The minutia with the second smallest distance to the root becomes the second minutia in the ordered sequence. This process continues until the minutia with maximum distance to the root becomes the last minutia in the ordered sequence. If the root-distance of two minutiae or more is equal, the angle of these minutiae is compared. The minutia with the smallest relative angle value becomes the next minutia in the ordered sequence.

NOTE –
To compute the position of the center of mass of a list of minutiae, the minutiae are considered as objects in a two-dimensional plane acting together as a single entity. The location of the centre of mass can be calculated if the mass m_i and location (x_i, y_i) of each component is known. By definition the centre of mass is located at (x_{com}, y_{com}) where

$$x_{com} = (m_1x_1 + m_2x_2 + ...) / (m_1 + m_2 + ...)$$
$$y_{com} = (m_1y_1 + m_2y_2 + ...) / (m_1 + m_2 + ...)$$

In the case of a minutiae list, all minutiae are considered equally weighted, which reduces the computation to (assume n minutiae).

$$x_{cm} = (x_1 + x_2 + ... + x_n) / n$$
$$y_{cm} = (y_1 + y_2 + ... + y_n) / n$$

9 CBEFF Format Owner and Format Types

Format owner and format type are encoded according to CBEFF. The format owner is ISO/IEC JTC 1/SC 37. The IBIA registered format owner id is ’0101’.

The format type denotes one of the finger minutiae formats according to this standard, see Table 18.

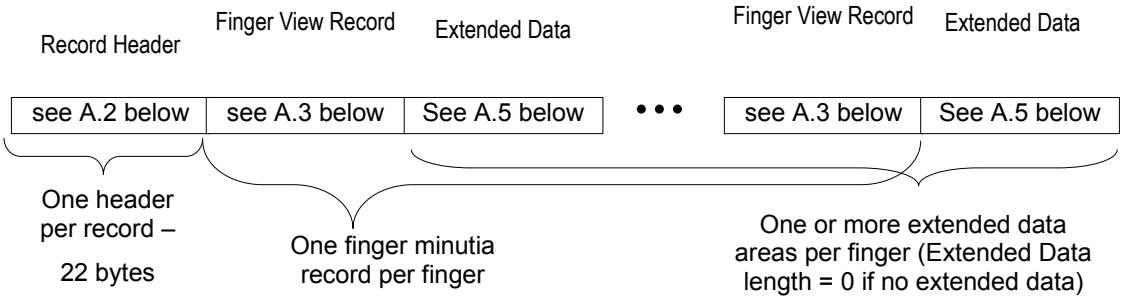
Table 18 — Format types

Format Type	Meaning
´0201´	Finger minutiae record format – no extended data, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton birfurcation points)
´0202´	Finger minutiae record format – extended data, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton birfurcation points)
´0203´	Finger minutiae card format - normal size, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton birfurcation points)
´0204´	Finger minutiae card format - normal size, with - ridge skeleton end points - ridge bifurcations (ridge skeleton birfurcation points)
´0205´	Finger minutiae card format - compact size, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton birfurcation points)
´0206´	Finger minutiae card format - compact size, with - ridge skeleton end points - ridge bifurcations (ridge skeleton birfurcation points)

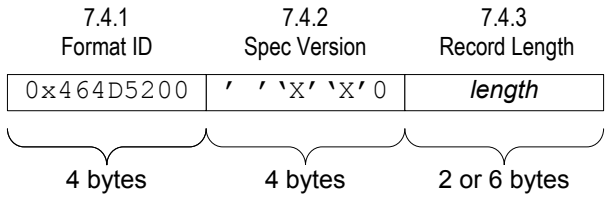
Annex A
(normative)

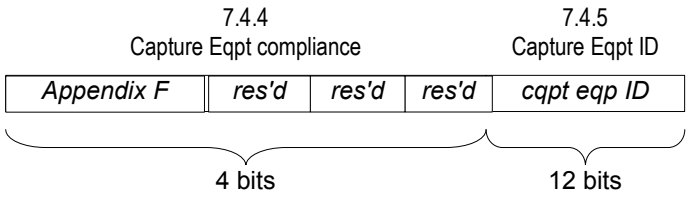
Record Format Diagrams

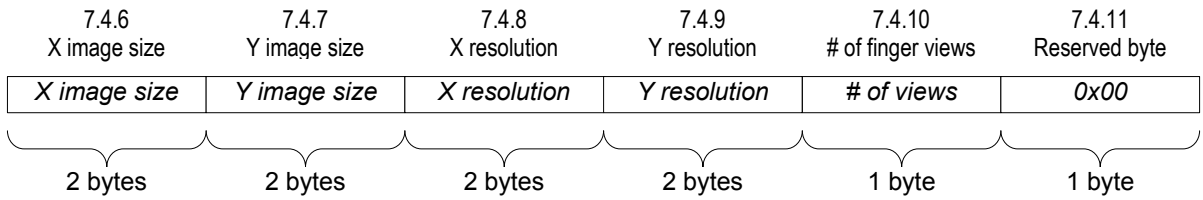
A.1 Overall Record Format



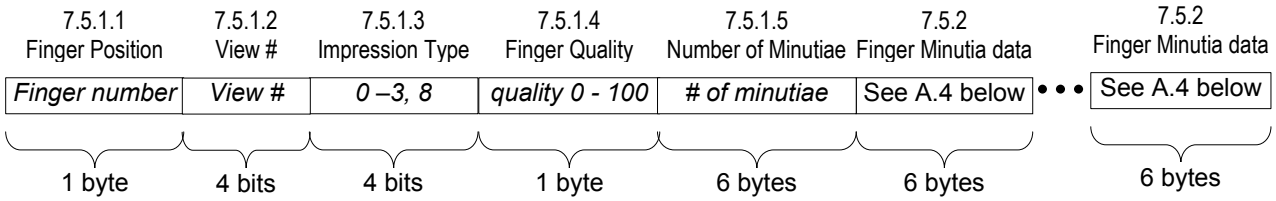
A.2 Record Header



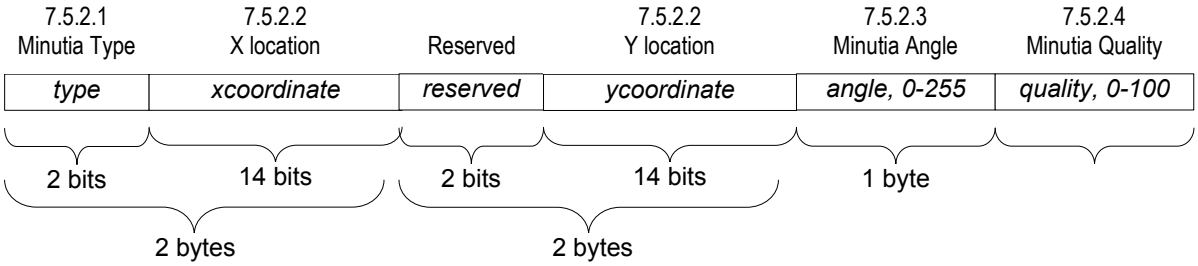




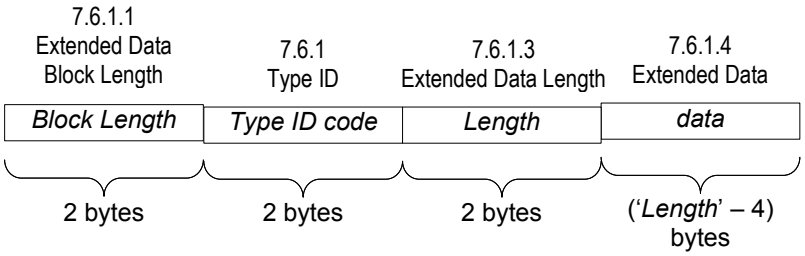
A.3 Single Finger View Minutiae Record



A.4 Finger Minutiae Data



A.5 Extended Data



Annex B
(informative)

Example Data Record

This example minutiae record demonstrates the format for a given set of data.

B.1 Data

Scanner ID = 0x00B5 (these values are determined by the IBIA - for the Vendor ID - and by the vendor)

Sensor Resolution: 500 dpi in both X and Y axes; 196.85 pixels per cm, Image was 512 by 512 pixels

Plain live-scan prints of the left and right index fingers

Left Index: Finger quality is 90% of the maximum possible; 27 minutia, listed in table below; no private feature data

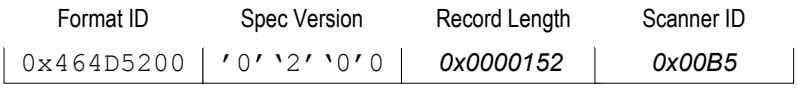
Right Index: Finger quality is 70% of the maximum possible; 22 minutia, listed in table below. Private feature data area (Type 01) consisting of six bytes: 0x01, 0x44, 0xBC, 0x36, 0x21, 0x43

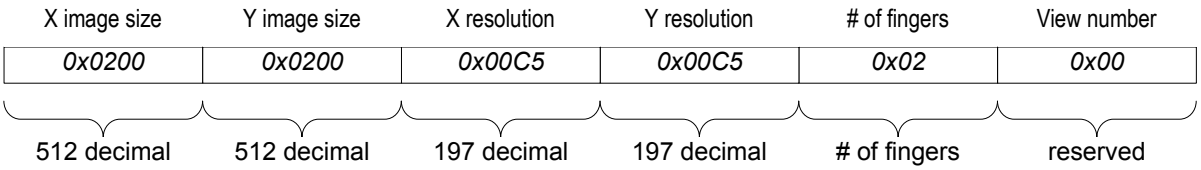
Record length = 340 = 26 (record header) + 2 * 4 (finger headers) + 27 * 6 (minutia for 1st finger) + 22 * 6 (minutia for 2nd finger) + 2 (null private area for 1st finger) + 10 (private area for 2nd finger)

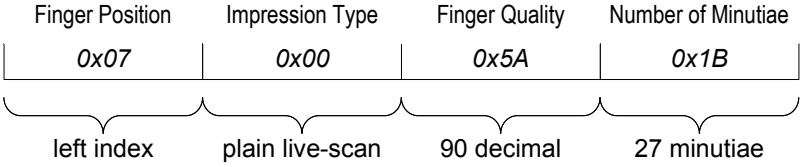
Minutia	Left Index Finger					Right Index Finger				
#	Type	X	Y	Angle	quality	Type	X	Y	Angle	quality
0	Ending	100	14	112	90	ending	40	93	0	90
1	Ending	164	17	85	80	bifurcation	116	100	0	80
2	Bifurcation	55	18	22	90	ending	82	95	12	70
3	Bifurcation	74	22	76	60	bifurcation	140	113	15	70
4	Ending	112	22	90	80	ending	122	135	18	80
5	Bifurcation	42	31	44	90	bifurcation	55	72	21	50
6	Bifurcation	147	35	51	90	ending	94	74	24	60
7	Ending	88	38	165	40	ending	155	62	42	80
8	Bifurcation	43	42	4	80	bifurcation	42	64	55	70
9	Ending	56	48	33	70	ending	155	85	59	80
10	Ending	132	49	72	90	bifurcation	96	192	62	80
11	Bifurcation	71	50	66	80	ending	114	86	85	80
12	Other	95	51	81	90	bifurcation	142	90	90	70
13	Ending	112	53	132	50	ending	57	137	100	90
14	Bifurcation	135	58	32	80	ending	131	75	110	80
15	Other	41	60	59	70	ending	45	113	120	80
16	Bifurcation	67	62	145	90	bifurcation	111	171	130	50
17	Ending	91	63	132	80	ending	95	62	150	60
18	Ending	112	65	33	60	bifurcation	61	114	200	80
19	Ending	53	71	45	90	bifurcation	143	72	250	80
20	Bifurcation	104	74	12	80	ending	63	104	300	70
21	Ending	75	79	21	90	bifurcation	125	73	350	40
22	Bifurcation	48	80	92	90					
23	Ending	130	89	45	80					
24	Bifurcation	63	95	126	80					
25	Ending	47	108	164	90					

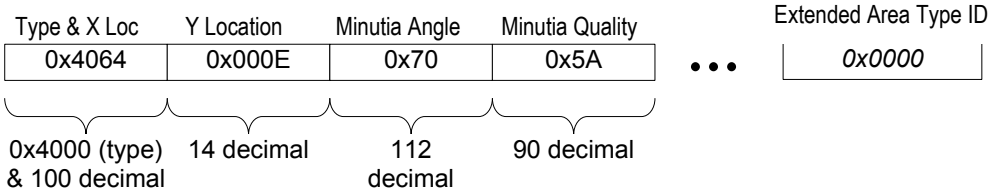
26	Bifurcation	126	115	172	30					

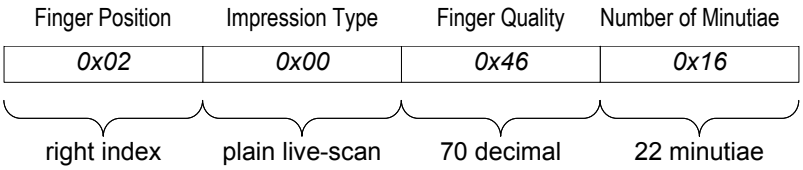
B.2 Example Data Format Diagrams

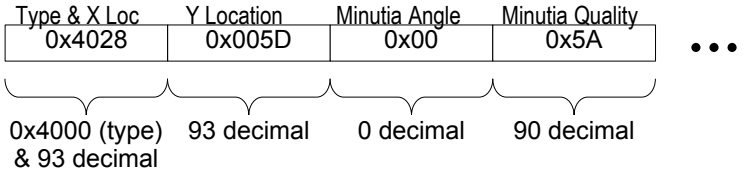


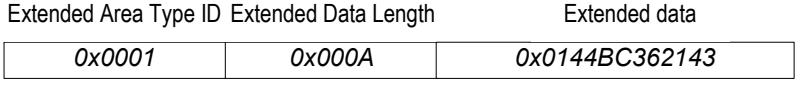












B.3 Raw Data for the Resulting Minutiae Record

Record Header:

0x464D520030323000015200B50200020000C500C50200

1st Finger Header:

0x07005A1B

1st Finger Minutiae data:

0x4064000E505A	0x40A400113C50	0x80370012105A
0x804A0016363C	0x407000164050	0x802A001F1F5A
0x80930023245A	0x405800267528	0x802B002A0350
0x403800301746	0x40840031335A	0x804700322F50
0x005F00333A5A	0x407000355E32	0x8087003A1750
0x0029003C2A46	0x8043003E675A	0x405B003F5E50
0x40700041173C	0x40350047205A	0x8068004A0950
0x404B004F0F5A	0x80300050415A	0x408200592050
0x803F005F5A50	0x402F006C755A	0x807E00737A1E

1st Private Data Area:

0x0000

2nd Finger Header:

0x02004616

2nd Finger Minutiae data:

0x4028005D005A	0x807400640050	0x4052005F0946
0x808C00710B46	0x407A00870D50	0x803700480F32
0x405E004A113C	0x409B003E1E50	0x802A00402746
0x409B00552A50	0x806000C02C50	0x407200563C50
0x808E005A4046	0x40390089475A	0x4083004B4E50
0x402D00715550	0x806F00AB5C32	0x405F003E6B3C
0x803D00728E50	0x808F0048B250	0x403F0068D546
0x807D0049F928		

2nd Private Data Area:

0x0001000A0144BC362143

Annex C
(informative)

Handling of Finger Minutiae Card Formats

C.1 Enrollment

C.1.1 Number of minutiae

The number of minutiae is a security sensitive parameter and depending on the security policy of the application. Persons who do not meet the minimum required number for enrolment cannot be enrolled. The maximum number of minutiae for the reference data is implementation dependent.

The recommended minimum number of minutiae required for enrollment is 16 and for verification is 12. The strength of function (see note at the end of this clause) may have impact on these values.

The maximum number of minutiae to be sent to a card is implementation dependent and related to:

- transmission time
- memory resources
- execution time
- security aspects

The recommended maximum value for enrollment and verification is 60. It is up to the extraction device to limit the number of minutiae sent to the card to 60 or the indicated value (see CBEFF Annex G, Table G.1).

NOTE - In the Common Criteria, the following definitions are given:

Strength of Function (SOF) — A qualification of a Target of Evaluation (TOE) security function expressing the minimum efforts assumed to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic — A level of TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium — A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high — A level of TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

C.1.2 Number of required finger presentations

The number of required finger presentations during an enrollment process is enrollment system dependent.

C.2 Matching

The verification data is subject to translation (in x- and y-direction), rotation (deviation of the orientation) and distortion. Matching also has to take into account components or factors like FAR/FRR.

C.2.1 Matching conditions

The result of the matching process is a score, which may denote the number of matching minutiae or any other appropriate value. In interoperability tests, it may be verified whether different implementations of the matching algorithm meet a required FAR/FRR e.g. in relation to the strength of function for the respective application.

If minutia types are taken into account in the matching process, the different types match according to Table .

Table C.1 - Minutiae type matching

Type of verification minutiae	Match with type of reference minutiae
00	00, 01, 02
01	00, 01
02	00, 02
00 = other 01 = ridge ending (encoded as valley skeleton bifurcation point), or ridge skeleton end point, see note 02 = ridge bifurcation (encoded as ridge skeleton bifurcation point)	

NOTE – The alternatives depend on the format type.

C.2.2 Threshold Value

A verification decision result is positive (i.e. the user verification is successful), if the score S as matching result is greater or equal than the required threshold value T:

$S \geq T$

The threshold value depends on several factors or components such as

- Required False Acceptance Rate FAR
- Required False Rejection Rate FRR
- Matching conditions, see 7.2.1
- The amount of minutiae enrolled
- The amount of minutiae presented
- Strength of function.

The treatment of the threshold value is dependent on the implemented matching strategy. In the following an example of the calculation of a threshold value is presented.

The threshold value T considered in this example is a dynamic value to be calculated for each verification process and depends on:

- Ar: amount of minutiae in the reference data
- Av: amount of minutiae in the verification data
- Avmin: minimum amount of minutiae required in the verification data
- Avmax: maximum amount of minutiae in the verification data relevant for threshold computation
- Tmin: minimum threshold value, which denotes the minimum amount of minutiae to be matched for positive verification
- Tmax: maximum threshold value, which denotes the maximum required amount of minutiae to be matched for positive verification.

T is computed as follows:

$T = Tmin + (Ac – Avmin) * (Tmax – Tmin)/(Avmax – Avmin)$

with

$Ac = qAr + (1 – q)Av,$

whereby Ac is the calculated amount of minutiae and the qualifier q the weight for Ar and Av

and

Avmin = min. amount of minutiae to be presented in a verification process

Avmax = max. amount of minutiae considered relevant in a verification process.

The values of Tmax, Tmin, Avmax, Avmin and q chosen for this example are shown in .

Table C.2 - Values for threshold computation (example)

Qualifier q	Tmin	Tmax	Avmin	Avmax
0.66	6	12	12	60

The values in Table A.1 together with the above formula have the following meaning:

- the amount of the reference minutiae have more significance than the amount of the verification minutiae (2/3 to 1/3)
- a score of 4 matching minutiae is generally rejected and leads to a negative verification result (S < T, Tmin required = 6)
- a score of 5 matching minutiae leads to positive verification (S ≥ T), if the respective person has a minimum of verification minutiae (12)

- a score of 12 matching minutiae leads in any case to a positive verification (Tmax required = 12).

NOTE: At court, some countries require 12 matching minutiae. However, the application area, the environment conditions and security requirements are different at court and for on-card-matching.

C.2.3 Retry Counter

For on-card matching, a retry counter (which is decremented by subsequent negative verifications and set to its initial value by positive verification) has to be implemented in order to limit the number of trials. The following aspects have impact on the initial value:

- experience of the user
- environmental conditions (e.g. construction of sensor embedding and finger placement)
- quality of verification data
- strength of function.

If the retry counter has reached the value 0, then the respective biometric verification method is blocked. Resetting the retry counter to its initial value is possible, if supported, e.g. by using the RESET RETRY COUNTER command (see ISO/IEC 7816-4) with a resetting code (8 digits).

The recommended initial value of the retry counter lies in the range of 5 and 15. The security policy of the application provider and the required strength of function have impact on the possible range and the value applied.

C.3 Security Aspects of Finger Minutiae Presentation to the Card

Fingerprints are left everywhere and therefore this kind of biometric data are considered to be public. An attacker may succeed in getting a good fingerprint of a person, derive from them the biometric verification data and present it to the stolen card of the respective person. To avoid this kind of attack and also replay attacks of data used in a previous verification process, a trusted path between card and service system is required. Such a trusted path is achieved by cryptographic means, e.g. using secure messaging according to ISO/IEC 7816-4. The specification of those secure messaging functions is usually application dependent and outside the scope of this standard.

Bibliography

[1] ANSI/NIST ITL 1-2000 „Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information" (NIST Special Publication 500-245)

[2] A. Jain, S. Pankanti: "Fingerprint Classification and Matching", Michigan State University, 1999 <need a better citation>

[3] S. Pankanti, S. Prabhakar, A. Jain: „On the Individuality of Fingerprints", in IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002

[4] AAMVA Driver License Standard 20000630 — Annex C: Finger Imaging, 2000

[5] ISO/IEC FDIS 7816-4:2003, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange.*

[6] ISO/IEC FDIS 7816-6:2003, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange.*

[7] ISO/IEC FDIS 7816-11:2003, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods.*

[8] ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER); Technical Corrigendum 2*

Annex D

ISO/IEC WD 19794-4: Biometric data interchange formats

Please see Annex D, in Appendix I.