



SEPTIÈME QUESTION À L'ORDRE DU JOUR

**Suivi de la convention (n° 185)
sur les pièces d'identité des gens de mer
(révisée), 2003**

1. A sa 288^e session, en novembre 2003, le Conseil d'administration a examiné un document établi par le Bureau sur le suivi de la convention sur les pièces d'identité des gens de mer (révisée), 2003, et sur les résolutions correspondantes adoptées par la Conférence internationale du Travail en juin 2003. Dans ce document¹, le Bureau évoquait les mesures à prendre d'urgence sur deux points qui pourraient inciter les gouvernements à ratifier rapidement la convention. L'un des deux aspects était l'élaboration d'une norme interopérable au plan mondial pour le «modèle biométrique fondé sur une empreinte digitale traduite sous forme de chiffres dans un code-barres» qui est prescrit par la convention. En novembre dernier, le Conseil d'administration a approuvé un plan proposé par le Bureau à la suite d'une réunion informelle tenue en septembre 2003, réunion qui regroupait des experts gouvernementaux et des représentants des armateurs et des gens de mer, ainsi que des organisations internationales compétentes. Conformément à ce plan, le Bureau a pris des dispositions en vue de l'élaboration rapide d'un rapport technique contenant la norme interopérable au plan mondial, qui est reproduite dans les annexes au présent document. Pour les raisons données ci-dessous, cette norme est présentée sous deux versions correspondant à deux formules différentes, l'annexe I, intitulée *Profil biométrique créé à partir du dessin papillaire digital aux fins de l'établissement des pièces d'identité des gens de mer*, et l'annexe II, intitulée *Profil biométrique créé à partir des minuties digitales aux fins de l'établissement des pièces d'identité des gens de mer*.
2. Le rapport technique présente la norme interopérable au plan mondial prescrite par la convention. En suivant cette norme, tous les pays émettant des pièces d'identité des gens de mer (PIM) seront à même de produire le même gabarit des empreintes digitales de l'intéressé et d'inscrire ce gabarit dans un code-barres imprimé sur la PIM. Par ailleurs, tous les pays visités par les gens de mer seront en mesure de lire de manière exacte le code-barres, ce qui leur permettra de s'assurer que l'intéressé est bien le détenteur de la PIM. Si le Bureau est à même de garantir cette interopérabilité avec une grande certitude, c'est pour trois raisons: *a)* la qualité du rapport technique; *b)* la compétence des personnes qui ont supervisé l'établissement de ce rapport; *c)* le caractère manifestement opportun des différentes mesures à prendre en vertu de l'établissement de la norme.

¹ Voir document GB.288/3/2.

3. En ce qui concerne le point *a*), le cabinet qui a établi le rapport était chaudement recommandé par un représentant d'un gouvernement qui participe à l'élaboration de la présente norme. Les coauteurs ont tous deux rempli au sein du gouvernement en question diverses fonctions liées aux pièces d'identité et à la biométrie. Leur cabinet offre des services de consultation techniques indépendants en matière de techniques d'authentification et est étroitement associé à l'élaboration des normes internationales relatives aux systèmes biométriques, notamment des normes qui sont soumises à l'approbation de l'Organisation internationale de normalisation (ISO). De fait, le rapport technique a été établi de manière à présenter une proposition de nouvelle norme à soumettre en temps utile à l'approbation de l'ISO.
4. En ce qui concerne le point *b*), le rapport technique prend en considération les indications et avis donnés par de nombreux représentants gouvernementaux qualifiés avant et durant l'établissement du rapport, ainsi que par des experts de l'ISO. Le Bureau est particulièrement reconnaissant à ces experts du soin avec lequel ils ont bien voulu examiner les projets de rapport.
5. S'agissant du point *c*), le caractère opportun des diverses mesures à prendre en vertu de la norme ressort de la manière claire dont le rapport technique se réfère aux bases sur lesquelles reposent ces mesures. Ces bases sont tout d'abord les conditions préalables qui sont énoncées dans la convention elle-même et sont analysées en profondeur dans la section 5.1 des deux versions du rapport technique, qui figurent en annexe au présent document. Ce sont également les normes techniques de l'Organisation de l'aviation civile internationale (OACI) visées dans la convention, ainsi que les normes techniques applicables qui ont été déjà élaborées ou sont à un stade d'élaboration avancé dans le cadre de l'ISO. La créativité du rapport technique tient donc essentiellement au fait qu'il regroupe en un tout cohérent les diverses procédures techniques qui sont déjà en vigueur et sont indiscutablement les mieux à même de permettre la bonne application des fonctions prescrites par la norme.
6. Un point, cependant, a donné lieu à de vives divergences d'opinion entre les experts consultés. Il s'agit de la manière dont la série de chiffres du gabarit devant être représentée dans le code-barres est tirée de l'image d'une empreinte digitale. Il existe deux méthodes qui font toutes deux l'objet de normes en cours de mise au point définitive dans le cadre de l'ISO: la méthode du *dessin papillaire*, dans laquelle le gabarit est déterminé par le tracé géométrique des crêtes du doigt, et la méthode des *minuties*, dans laquelle le gabarit est déterminé par le nombre et la position des minuties (coupures et bifurcations) que l'on trouve sur les crêtes. Compte tenu de cette divergence d'opinion, le Bureau a envoyé en décembre 2003 une demande d'informations à ce sujet aux gouvernements de tous les Etats Membres et un questionnaire aux entreprises qui fournissent les technologies et matériels correspondants. Au 11 février 2004, 28 réponses avaient été reçues des gouvernements à la question relative aux aspects technologiques. Douze pays (dont deux grands pays fournisseurs de main-d'œuvre) exprimaient une préférence pour les gabarits créés à partir des *minuties*, 13 n'exprimaient aucune préférence et trois se déclaraient favorables à la méthode recourant au *dessin papillaire*.
7. En raison de la divergence d'opinion évoquée ci-dessus, le rapport technique qui accompagne le présent document est soumis sous deux versions correspondant aux deux grandes options: l'un (ILO SID-0001) présente la technologie faisant appel au *dessin papillaire* (annexe I) et l'autre (ILO SID-0002) présente la technologie faisant appel aux *minuties* (annexe II). La section 5.1.4 de la première version (ILO SID-0001) explique les raisons pour lesquelles l'option fondée sur le *dessin papillaire* a été retenue, de préférence à l'option fondée sur les *minuties*, et celle de la seconde version (ISO SID-0002) explique les raisons pour lesquelles l'option fondée sur les *minuties* a été retenue, de préférence à l'option fondée sur le *dessin papillaire*. Pour les raisons indiquées ci-dessous, il apparaît

clairement que cette dernière méthode, qui est en fait celle qui avait été recommandée par les participants à la réunion de septembre 2003, mentionnée au paragraphe 1 ci-dessus, répondrait mieux aux prescriptions de la convention. La méthode fondée sur les *minuties* présente le double avantage d'être mieux connue des gouvernements utilisant la norme et d'être plus facilement intégrable aux autres systèmes nationaux recourant à la technique des empreintes digitales, particulièrement en ce qui concerne les enquêtes criminelles.

8. D'un point de vue technique, les deux méthodes conviennent bien à un système interopérable visant à s'assurer avec certitude que le détenteur de la pièce d'identité est bien le marin à qui elle a été délivrée. Il existe cependant une marge d'incertitude due au fait que, si l'on retient la méthode fondée sur les *minuties*, seule une certaine quantité d'informations peut être stockée dans le code-barres des PIM. Les experts s'entendent généralement pour admettre que les informations devraient concerner les deux empreintes digitales (de façon, s'il n'est pas possible de prendre d'empreinte d'un doigt au moment de la vérification ou si l'image de ce doigt n'est pas suffisamment claire, à pouvoir prendre une empreinte d'un autre doigt). Les informations obtenues en appliquant les normes en vigueur pourront toujours être stockées dans le code-barres si l'on choisit la méthode fondée sur le *dessin papillaire*. En revanche, si l'on opte pour la méthode fondée sur les *minuties*, il y aura des cas où le nombre de minuties des doigts examinés fourniront des informations dépassant la capacité du code-barres. La solution simple serait alors de réduire le nombre des minuties à prendre en considération, et c'est pourquoi le document ILO (SID-0002, qui figure en annexe, expose une manière satisfaisante de procéder à cette opération (voir la section 5.1.3, deuxième paragraphe). Cependant, comme cette «amputation» n'a fait l'objet d'aucune norme testée, on ne peut savoir avec certitude au stade actuel si l'on obtiendrait toujours le même gabarit.
9. De manière plus générale, en fait, la méthode fondée sur le *dessin papillaire* présente à ce stade davantage de fiabilité. Les normes internationales relatives aux deux méthodes en sont encore à l'étape du projet (quoiqu'à un stade avancé). Les produits conformes au projet de norme fondé sur le *dessin papillaire* ont été testés officiellement par des tiers indépendants, tandis que les produits réputés conformes au projet de norme fondé sur les *minuties* ne l'ont pas été. Comme l'indiquent les réponses au questionnaire envoyé aux vendeurs, lorsque la norme internationale aura été parachevée et que les clients exigeront que les produits soient conformes à cette norme, les vendeurs de produits fondés sur les *minuties* pourraient être tenus d'apporter les changements voulus à ces produits. Cependant, comme dans le cas de toute amélioration technologique de ce type, il faudra procéder à des tests indépendants des produits fondés sur les *minuties* (y compris en ce qui concerne les effets de l'«amputation» exigés par le gabarit de la PIM), afin de s'assurer que les changements apportés ne nuisent pas à l'efficacité des différents produits ou n'ont pas pour effet imprévu de rendre le système vulnérable.
10. Aux termes du paragraphe 8 c) de l'article 3 de la convention, «le matériel nécessaire au recueil et à la vérification des données biométriques [doit être] facile à utiliser et [être] généralement accessible aux gouvernements à faible coût». Selon ce critère, la méthode fondée sur le *dessin papillaire* apparaît légèrement préférable, car elle permet d'exploiter efficacement une image de résolution plus faible que celle exigée par l'autre méthode. On pourrait donc utiliser un matériel moins coûteux pour obtenir l'image de l'empreinte digitale durant les opérations d'émission de la PIM et la vérification ultérieure de l'identité du détenteur. Cependant, un gouvernement a indiqué qu'il faudrait utiliser à cette fin des détecteurs optiques (quoiqu'ils ne soient pas exigés si l'on choisit la méthode biométrique fondée sur le *dessin papillaire*), parce que, selon la réponse, un tel matériel résisterait mieux à l'environnement marin. Un autre facteur pouvant influencer sur le coût du matériel tient au fait que, s'il existe un certain nombre de consultants, d'ensembliers et de fabricants de matériel qui recourent à la technologie fondée sur le *dessin papillaire*, le nombre des fournisseurs de technologies fondées sur les *minuties* est beaucoup plus élevé, et ces

fournisseurs disposent de leurs propres consultants, assembleurs de systèmes et fabricants. Cependant, avant de procéder à des tests officiels indépendants des produits pour faire la preuve de leur conformité avec le projet de norme internationale et de l'applicabilité de ce projet de norme, les acheteurs de matériel correspondant à l'option *minuties* pourront avoir à dépendre d'un nombre restreint de vendeurs, et peut-être même d'un vendeur unique.

11. Une faiblesse manifeste de la méthode fondée sur les *minuties* tient au fait qu'elle risque de ne pas être conforme à la prescription de la convention (art. 3, paragr. 8 *b*)), selon laquelle «les données biométriques [ne doivent pas pouvoir] être reproduites à partir du modèle ou d'autres représentations». Des publications mentionnent des méthodes permettant de contrefaire les empreintes digitales obtenues grâce au gabarit fondé sur les *minuties*. Il n'existe aucune publication similaire pour la méthode fondée sur le *dessin papillaire*.
12. Un gouvernement dont les systèmes seraient fondés sur les *minuties* n'aurait pas de difficulté particulière à exploiter un programme fondé sur le *dessin papillaire* pour produire et vérifier le gabarit des empreintes digitales (de la même façon que plusieurs programmes totalement différents peuvent se dérouler simultanément sur le même ordinateur). Cependant, un gabarit fondé sur le *dessin papillaire* ne pourrait être utilisé pour effectuer des recherches dans les bases de données dans lesquelles les empreintes digitales sont stockées uniquement sous forme de gabarit fondé sur les *minuties*, ce qui peut être en particulier le cas des bases de données nationales relatives aux enquêtes criminelles. Or l'utilisation des gabarits pour toute autre fin que la vérification de l'identité des gens de mer n'est pas conforme à l'esprit de la convention, comme l'indiquent diverses dispositions, par exemple le paragraphe 7 de l'article 4, aux termes duquel «les Membres doivent faire en sorte que les données personnelles saisies dans la base de données électronique ne soient pas utilisées à d'autres fins que celles de vérifier les pièces d'identité des gens de mer».
13. Ainsi, sans vouloir préjuger des avantages généraux de la méthode fondée sur les *minuties*, le Bureau conclut que la méthode fondée sur le *dessin papillaire* devrait être retenue, car c'est elle qui répond le mieux aux prescriptions et aux intentions de la convention sur les pièces d'identité des gens de mer. A cet égard, il y a lieu de noter que le but de cette convention n'est pas de mettre en place la solution idéale. De fait, il a été expressément décidé de ne pas appliquer la solution la plus efficace, qui consiste à recourir à une image biométrique stockée sur une microplaquette. Le but essentiel est triple: disposer d'une solution biométrique qui soit à la fois relativement peu coûteuse et acceptable et qui puisse être utilisée durant les cinq premières années (ou plus) de la durée d'application de la convention; disposer d'un outil complétant efficacement les autres données personnelles prescrites par la convention, comme la signature et la photographie; pouvoir exploiter rapidement cette solution sans précédent. Quoique la norme exposée dans le rapport technique doive encore faire l'objet de tests dans un laboratoire de certification², il a été suggéré que le Conseil d'administration donne son approbation dès maintenant. Les Membres susceptibles de ratifier la convention pourront ainsi se faire une idée claire des prescriptions relatives à ce point. Toute modification concernant des points de détail pourrait être faite ultérieurement.
14. ***Au vu de ce qui précède, le Conseil d'administration voudra sans doute:***
 - a) ***retenir l'option fondée sur le dessin papillaire, comme le recommande le Bureau, et approuver le document ILO SID-0001 (annexe I du présent document), qui définit la norme applicable au modèle biométrique des***

² Voir document GB.288/3/2, paragr. 8.

empreintes digitales prescrit par le paragraphe k) de l'annexe I de la convention sur les pièces d'identité des gens de mer (révisée), 2003; ou

- b) retenir l'option fondée sur les minuties et approuver le document ILO SID-0002 (annexe II du présent document), qui définit la norme applicable au modèle biométrique des empreintes digitales prescrit par le paragraphe 4 de l'annexe I de la convention sur les pièces d'identité des gens de mer (révisée), 2003.*

Genève, le 24 février 2004.

Point appelant une décision: paragraphe 14.

Annexe I

Profil biométrique créé à partir du dessin papillaire digital aux fins de l'établissement des pièces d'identité des gens de mer

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

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

Page

Table des matières

Avant-propos	2
0. Introduction	3
0.1. Principes de base de l'élaboration des documents.....	3
0.2. Travaux connexes.....	4
0.3. Détermination de l'option biométrique fondée sur les empreintes digitales	5
1. Champ d'application	5
2. Conformité	7
3. Références	7
3.1. Normes contraignantes	7
3.2. Documentation	8
3.3. Normes et documents complémentaires à élaborer ou à privilégier en vue d'une utilisation par les gens de mer.....	8
4. Définitions	8
4.1. Termes et définitions	8
5. Conditions que doit remplir le système biométrique permettant l'établissement des PIM	11
5.1. Conditions que doit remplir le système biométrique d'établissement des PIM à partir du dessin papillaire digital	11
5.2. Prescriptions relatives au code-barres utilisé sur les PIM	17
5.3. Prescriptions relatives à la vérification des données biométriques des PIM	19
5.4. Prescriptions relatives aux bases de données concernant les PIM	20

Annexe A: SID pattern-based fingerprint bar code format (normative)

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

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

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

Avant-propos

L'Organisation internationale du Travail, créée en 1919, est une institution spécialisée des Nations Unies. C'est un organisme tripartite, au sein duquel les représentants des gouvernements, des employeurs et des travailleurs sont placés sur un pied d'égalité. En juin 2003, l'OIT a adopté la convention n° 185 sur les pièces d'identité des gens de mer (révisée). La révision de la convention précédente, laquelle datait de 1958, a été motivée par les débats tenus au sein de l'Organisation maritime internationale (OMI) en vue d'examiner les mesures et règles propres à prévenir les actes de terrorisme qui menacent la sécurité des passagers et des équipages, ainsi que la sûreté des navires. La nouvelle convention de l'OIT a été communiquée aux gouvernements des Etats Membres de l'Organisation pour examen en vue de sa ratification. Elle aura un caractère obligatoire, au même titre qu'un traité international, pour tous les Membres qui l'ont ratifiée.

Le Bureau international du Travail, qui est le secrétariat de l'Organisation, a chargé les auteurs du présent document d'établir un projet de rapport technique qui constituera la base d'une norme à soumettre ultérieurement à l'ISO en vue d'obtenir son aval, cette norme portant sur un modèle biométrique interopérable conforme aux dispositions de la convention n° 185 et couvrant les domaines suivants: saisie des données relatives aux empreintes digitales, création de gabarits et stockage des codes-barres. Le rapport fera état des techniques et procédures les mieux adaptées dans les domaines suivants: imprimerie, lecture, enrôlement, format des codes-barres, détecteurs/lecteurs biométriques, considérations relatives aux bases de données et format d'un modèle biométrique interopérable au plan mondial. Le rapport devrait également prendre en considération les questions relatives aux bases de données concernant la qualité et l'interopérabilité.

L'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) constituent le système spécialisé de la normalisation mondiale. Les organes nationaux qui sont membres de l'ISO et de la CEI participent à l'élaboration des normes internationales dans le cadre des comités techniques créés par l'organisation compétente pour traiter des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent à des questions d'intérêt mutuel. D'autres organisations internationales, tant gouvernementales que non gouvernementales, participent également à ces travaux, en liaison avec l'ISO et la CEI.

Les normes internationales sont rédigées selon les règles énoncées à la partie 2 des directives de l'ISO et de la CEI.

Dans le domaine de l'informatique, l'ISO et la CEI ont créé un comité technique conjoint, qui transmet pour approbation aux organes nationaux les projets de normes internationales qu'il a adoptés.

Le présent rapport (ILO SID-0001), intitulé *Profil biométrique créé à partir du dessin papillaire digital aux fins de l'établissement des pièces d'identité des gens de mer*, a été élaboré par le Bureau international du Travail. Il peut être soumis en tant que contribution technique au comité conjoint ISO/CEI JTC 1 SC37, *Biométrie*. Il se divise en cinq sections, à savoir:

- section 1 – Champ d'application;
- section 2 – Conformité;
- section 3 – Références;

- section 4 – Termes et définitions;
- section 5 – Conditions que doit remplir le système biométrique permettant l'établissement des PIM.

La section 5 se subdivise elle-même en quatre sous-sections, à savoir:

- section 5.1. – Conditions que doit remplir le système biométrique d'établissement des PIM à partir du dessin papillaire digital;
- section 5.2. – Prescriptions relatives au code-barres utilisé sur les PIM;
- section 5.3. – Prescriptions relatives à la vérification des données biométriques des PIM;
- section 5.4. – Prescriptions relatives aux bases de données concernant les PIM.

0. Introduction

0.1. Principes de base de l'élaboration des documents

A la suite des attaques terroristes du 11 septembre 2001, l'Organisation internationale du Travail a pris des mesures pour réviser la convention (n° 108) sur les pièces d'identité des gens de mer, 1958, selon une procédure accélérée. Le nouvel instrument, à savoir la convention (n° 185) sur les pièces d'identité des gens de mer (révisée), 2003, qui a été adoptée par la Conférence internationale du Travail en juin 2003, propose des normes de sécurité modernes visant à résoudre la question urgente posée par le refus d'admettre les gens de mer sur le territoire des pays visités par leurs navires en vue de prendre un congé à terre, de passer en transit, de gagner un navire ou de changer de navire. L'une de ces normes de sécurité est un modèle biométrique correspondant à une empreinte digitale traduite sous formes de chiffres dans un code-barres «répondant à une norme à déterminer» (convention n° 185, annexe I).

Dans une résolution adoptée par la Conférence internationale du Travail en juin 2003, il a été demandé au Directeur général que les institutions compétentes «prennent rapidement des mesures en vue de l'élaboration d'une norme interopérable au plan mondial» sur le modèle biométrique mentionné ci-dessus, particulièrement en coopération avec l'Organisation de l'aviation civile internationale. Lors d'une réunion qui s'est tenue à l'OIT en septembre 2003, réunion à laquelle participaient les représentants des gouvernements, des armateurs et des gens de mer, ainsi que ceux de l'OACI et de l'ISO, il est apparu clairement que l'OACI, qui œuvre à l'élaboration d'une recommandation privilégiant une solution biométrique différente (voir ci-dessous) en tant que norme applicable aux passeports lisibles à la machine, n'était pas à même de prendre une part active à l'élaboration du modèle exigé par la nouvelle PIM. Il a été également noté que le temps limité dont on disposait avant l'entrée en vigueur de la convention n° 185 interdisait de recourir à la procédure normale d'élaboration d'un tel modèle dans le cadre de travail de l'ISO et de la CEI.

Aussi le BIT a-t-il commandé le présent rapport technique, intitulé ILO SID-0001 rev. 05, pour exposer les exigences strictes imposées par la convention n° 185 au sujet de l'identification personnelle des gens de mer par voie biométrique. Les auteurs soumettent ce rapport sous la forme d'un profil biométrique définissant la norme applicable à la création et au stockage de gabarits biométriques établis à partir du dessin papillaire digital dans le code-barres PDF417 des PIM de la prochaine génération et dans les bases de données électroniques nationales des Membres (voir respectivement annexes I et II à la

convention n° 185). Ce profil biométrique se présente sous une forme largement conforme à la norme de l'ISO et peut évoluer vers une norme, puis vers un document d'achat, à la suite d'une discussion internationale et d'une harmonisation des prescriptions.

0.2. Travaux connexes

Tout un ensemble d'études, d'expérimentations, de programmes pilotes et de produits ont été réalisés au cours des dernières années pour accélérer les opérations d'inspection aux points de passage des frontières. Nombre de travaux incorporent les techniques biométriques dans les documents de voyage et les pièces d'identité internationales de la prochaine génération. L'OIT a élaboré la convention n° 185 pour définir les normes des pièces d'identité des marins de la prochaine génération, qui contiendront des données d'identification personnelle du marin (détenteur du document) fondées sur la biométrie et stockeront des gabarits biométriques dans un code-barres imprimé.

Avant le 11 septembre 2001, le secteur de la biométrie avait lancé divers projets d'élaboration de normes pour faciliter la mise au point de produits et de systèmes biométriques interopérables, ainsi que l'échange de données biométriques entre les produits et les systèmes, et les normes à respecter pour garantir l'intégrité et la confidentialité des données biométriques.

- ISO/IEC FCD 19784 – Technologie de l'information – Interface relative au programme d'application biométrique (BioAPI) (ISO/IEC JTC 1 SC37 N numéro 55¹, datée du 17 décembre 2002), qui propose une interface de programmation de l'application garantissant que les produits et systèmes conformes peuvent interopérer entre eux (il s'agit aussi d'une norme de l'Institut américain de normalisation et de l'International Committee for Information Technology Standards: ANSI/INCITS 358:2002 – Technologies de l'information – Spécification BioAPI).
- ISO/IEC CD 19785 – Technologies de l'information – Cadre relatif aux formats d'échange biométriques communs (CBEFF) (ISO/IEC JTC1 SC37 N 208, datée du 14 juillet 2003).
- ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 3: données relatives au dessin papillaire digital (ISO/IEC JTC 1 SC37 N313, datée du 3 octobre 2003). (Il s'agit également d'une norme définitive ANSI/INCITS: ANSI/INCITS 377 – Format d'échange fondé sur le dessin papillaire digital.
- Norme de l'Organisation de l'aviation civile internationale (OACI) (document 9303) applicable aux documents de voyage à lecture optique, établie à la demande du comité technique ISO/IEC JTC1 SC17.

Note: La recommandation la plus récente de l'OACI consiste à inclure la technologie des cartes à puce sans contact dans les documents de voyage de la prochaine génération, ainsi qu'une ou plusieurs donnée(s) biométrique(s) (les données biométriques faciales sont prescrites par la norme MRTD de l'OACI, et l'on pourrait également inclure soit une empreinte digitale, soit un système de reconnaissance de l'iris. Bien que la PIM de l'OIT soit un document d'identité (et non un document de voyage), l'Organisation s'efforcera, dans la mesure du possible, de suivre le projet de norme de l'OACI relatif aux documents de voyage à lecture optique de la prochaine

¹ Pour consulter le document ISO/IEC JTC 1 SC37, consultez le site Internet www.jtcl.org, sélectionnez le sous-comité 37, allez dans la partie relative aux documents et tapez le numéro de document dans la zone N Number).

génération. Il est important de noter que les PIM de la prochaine génération utiliseront une technologie fondée sur les codes-barres pour stocker les données biométriques (et non la technologie faisant appel à des circuits intégrés incorporés, recommandée par la norme MRTD de l'OACI). Cette différence a des conséquences importantes pour le profil biométrique de la PIM. Si le système de stockage utilisant les codes-barres est moins coûteux que le système utilisant les circuits intégrés, le premier (SID PDF417) offre une capacité de stockage nettement moindre que le second.

Comme la PIM de l'OIT de la prochaine génération utilisera la technologie fondée sur les codes-barres pour stocker les données biométriques et répondre aux normes d'interopérabilité de ce document, ce profil biométrique définit le format du stockage des gabarits d'empreintes digitales utilisant le code-barres PDF417. Aussi les normes ISO/IEC 15438:2001 (symbologie du code-barres PDF417 et ISO/IEC FDIS 15415 (qualité d'impression correspondant au code-barres PDF 417) sont-elles fondamentalement applicables à ce profil biométrique?

Prises ensemble, ces différentes normes (ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 3: données relatives au dessin papillaire digital (ISO/IEC JTC 1 SC37 N 313, datée du 3 octobre 2003) et OACI 9303) représentent les fondations sur lesquelles il est possible d'édifier les moyens biométriques des systèmes relatifs aux PIM. D'autres normes déjà élaborées (comme la norme ANSI/INCITS 358:2002 – Technologies de l'information – Spécification BioAPI) ou en cours d'élaboration, parallèlement à cette norme (comme la norme ISO/IEC WD 19794-4 – Formats d'échange de données biométriques – Partie 4: format d'échange fondé sur l'image des empreintes digitales (ISO/IEC JTC 1 SC37 N 341, datée du 7 octobre 2003) présenteront également une utilité (voir ci-dessous).

0.3. Détermination de l'option biométrique fondée sur les empreintes digitales

La convention n° 185 de l'OIT dispose que la PIM doit être interopérable sur le plan international. Aussi l'OIT devait-elle choisir entre les données biométriques fondées sur l'image, les *minuties* ou le *dessin papillaire* comme base de la pièce d'identité des marins de la prochaine génération. Deux rapports techniques ont été établis, et les comités techniques correspondants ont donné leur avis à l'appui de la décision de l'Organisation. Le présent rapport (SID-0001) expose les prescriptions techniques de l'option biométrique fondée sur le *dessin papillaire*, option qui a été retenue parce qu'elle représente la solution la mieux adaptée aux besoins de l'OIT, compte tenu des arguments avancés dans la section 5.1.3, intitulée *Saisie des empreintes digitales*.

L'OIT se réserve le droit de reconsidérer cette décision à mesure que les normes internationales et les options technologiques allant à l'appui de la convention n° 185 évoluent.

1. Champ d'application

Le présent rapport technique (ILO SID-0001), intitulé *Profil biométrique créé à partir du dessin papillaire digital aux fins de l'établissement des pièces d'identité des gens de mer*, donne des orientations en vue de l'incorporation des technologies biométriques fondées sur les caractéristiques des empreintes digitales dans les PIM, conformément à la convention (n° 185) sur les pièces d'identité des gens de mer (révisée), 2003. Les auteurs ont fait appel aux ressources complémentaires suivantes: 1) la note d'orientation relative au gabarit biométrique établie par la réunion informelle sur la biométrie en vue des PIM, qui s'est tenue les 29 et 30 septembre 2003; 2) des documents d'information

supplémentaires; 3) la réunion relative à une consultation technique qui s'est tenue à Genève du 5 au 7 décembre 2003; et 4) les avis d'experts du terrain.

La biométrie sera utilisée pour renforcer le lien existant entre la PIM et le marin qui la détient.

Le rapport est structuré comme suit: prescriptions relatives à la conformité du profil biométrique (section 2). Références techniques (section 3); Définitions (sections 4); Prescriptions biométriques relatives aux PIM (section 5). Cette dernière section se subdivise en quatre sous-sections:

- la sous-section 5.1, intitulée *Prescriptions biométriques établies à partir du dessin papillaire digital*, qui comprend l'enrôlement et la saisie des empreintes digitales, ainsi que le modèle d'empreinte digitale à incorporer dans les pièces d'identité des gens de mer de la prochaine génération;
- la sous-section 5.2, intitulée *Prescriptions relatives au code-barres utilisé sur les PIM*, qui comprend le format des codes-barres, la technique d'impression et les spécifications de cette impression, la technique de lecture et les caractéristiques physiques des codes-barres;
- la sous-section 5.3, intitulée *Prescriptions relatives à la vérification des données biométriques* des PIM, qui expose la procédure de vérification de l'identité biométrique;
- la sous-section 5.4, intitulée *Prescriptions relatives aux bases de données concernant les PIM*, qui expose les prescriptions relatives aux bases de données concernant les codes-barres et celles relatives aux bases de données électroniques nationales concernant les PIM.

L'annexe A expose en détail le format des codes-barres concernant les PIM. L'annexe B décrit le format des données biométriques relatives au dessin papillaire. L'annexe C comprend un exemplaire des normes suivantes: ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 3: Données relatives au dessin papillaire digital (ISO/IEC JTC 1 SC37 N 313, datée du 3 octobre 2003). L'annexe D comprend un exemplaire des normes suivantes: ISO/IEC WD 19794-4 – Formats d'échange des données biométriques – Partie 4: Format d'échanges fondé sur l'image des empreintes digitales (ISO/IEC JTC 1 SC37 N 341, datée du 7 octobre 2003).

Comme ce format de stockage des empreintes digitales a été élaboré en conformité avec les documents relatifs aux projets de normes ISO, le présent document primera pour ce qui est des pièces d'identité des gens de mer, au cas où l'évolution de l'un ou l'autre de ces projets de normes semblerait indiquer qu'ils sont en contradiction.

Les questions ci-dessous sont exclues du champ d'application du présent rapport technique:

- 1) processus d'ensemble relatif aux systèmes d'identification des gens de mer faisant appel aux techniques biométriques;
- 2) critères de validation de l'identité des gens de mer et de leur titre professionnel;
- 3) critères d'émission des PIM;
- 4) opportunité de faire appel à d'autres techniques biométriques fondées sur le dessin papillaire digital;

- 5) critères concernant «les autres caractéristiques relatives à la sécurité» qui sont mentionnées dans l'introduction à l'annexe I de la convention n° 185;
- 6) questions relatives à l'environnement marin, y compris celles qui concernent la corrosion saline (ces questions devraient toutefois être abordées dans le cadre des spécifications relatives à la fourniture des PIM);
- 7) évaluation des risques liés à l'application.

2. Conformité

Un système biométrique est conforme à la norme s'il satisfait à toutes les prescriptions obligatoires définies à la section 5, intitulée *Conditions que doit remplir le système biométrique d'établissement des PIM*, à l'annexe A, *SID pattern-based fingerprint bar code format*, et à l'annexe B, *SID bar code pattern-based fingerprint storage format*.

Toutes les techniques et caractéristiques biométriques ne conviennent pas aux pièces d'identité des gens de mer, compte tenu des exigences de l'OIT et du degré d'évolution des normes internationales relatives aux techniques biométriques applicables aux empreintes digitales à la date de la présente publication. La norme correspond aux prescriptions permettant d'obtenir l'interopérabilité internationale des composants biométriques des empreintes digitales fondés sur le dessin papillaire digital des pièces d'identité des gens de mer de la prochaine génération.

3. Références

Le présent profil biométrique est élaboré avant que n'ait été effectuée la mise au point définitive des projets de normes qui s'y rapportent. Tout projet de norme cité dans la présente section indique le numéro de document figurant dans la norme SC37 et la date de publication du projet dont il est question. Un exemplaire de tous les projets de *normes contraignantes* mentionnées (voir la section 3.1) est inclus en annexe au présent document. Comme ce format de stockage des empreintes digitales a été élaboré en conformité avec les documents relatifs aux projets de normes ISO, *le présent document primera pour ce qui est des pièces d'identité des gens de mer*, au cas où l'évolution de l'un ou l'autre de ces projets de normes semblerait indiquer qu'ils sont en contradiction.

3.1. Normes contraignantes

- a) ISO/IEC FCD 19784 – Technologies de l'information – Interface relative au programme d'application biométrique (BioAPI) (ISO/IEC JTC 1 SC37 N numéro 55, datée du 17 décembre 2002) (Il s'agit aussi d'une norme définitive ANSI/INCITS: ANSI/INCITS 358:2002 – Technologies de l'information – Spécification BioAPI.)
- b) ANSI/NIST-ITL 1-2000 – Format des données relatives à l'échange d'informations concernant les empreintes digitales – Tableau 5.
- c) ISO/IEC FDIS 15415 – Technologies de l'information – Techniques d'identification automatique et de saisie des données – Spécifications des tests de qualité de l'impression des codes-barres – Deux symboles dimensionnels.
- d) ISO/IEC 15438:2001 – Technologies de l'information – Techniques d'identification automatique et de saisie des données – Spécifications de la symbologie des codes-barres – PDF417.

- e) ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 3: Données relatives au dessin papillaire digital (ISO/IEC JTC 1 SC37 N 313, datée du 3 octobre 2002). (Il s'agit aussi d'une norme définitive ANSI/INCITS: ANSI/INCITS 377 – Format d'échange fondé sur le dessin papillaire digital.)
- f) ISO/IEC WD 19794-4 – Formats d'échange de données biométriques – Partie 4: Format d'échange fondé sur une image des empreintes digitales (ISO/IEC JTC 1 SC37 N 341, datée du 7 octobre 2003).
- g) ISO/IEC 8859-15:1999 – Technologies de l'information – Jeux de caractères graphiques codés sur un seul octet – Partie 15: Alphabet latin n° 9.
- h) ISO 3166-1:1997 – Codes de représentation des noms de pays et de leurs subdivisions – Partie 1: Codes de pays.
- i) ISO/IEC 9945-1:2003 – Technologies de l'information – Interface pour la portabilité des systèmes (POSIX) – Partie 1: Définitions de base.

3.2. Documentation

- j) Document de l'OACI 9303 – Documents de voyage à lecture optique (Partie 1, 5^e édition, 2003; Partie 3, 2^e édition, 2002).
- k) ANSI/NIST-ITL-1-2000, Format des données types pour l'échange d'informations relatives aux empreintes digitales, au visage, aux cicatrices et aux tatouages (SMT).
- l) ISO/IEC 7810:2003 – Cartes d'identification – Caractéristiques physiques.

3.3. Normes et documents complémentaires à élaborer ou à privilégier en vue d'une utilisation par les gens de mer

- m) Norme relative aux demandes d'octroi de PIM.
- n) Norme relative aux tests et aux déclarations concernant les performances et l'interopérabilité des PIM.
- o) Document d'orientation complet et facile à consulter sur la prise des empreintes digitales, en vue d'aider le personnel d'enrôlement et de vérification à produire des résultats cohérents et fiables.

4. Définitions

Les auteurs se sont efforcés de faire en sorte que les termes, définitions, symboles et abréviations utilisés dans le présent rapport technique soient conformes à la norme sur l'harmonisation du vocabulaire de la biométrie en cours d'élaboration au sein du groupe de travail 1 d'ISO/IEC JTC 1 SC 37. Certains termes utiles sont définis ci-après pour faciliter la lecture de ce document.

4.1. Termes et définitions

4.1.1. Profil d'application

Sous-ensembles conformes ou ensembles de normes de base utilisés pour exécuter certaines fonctions précises. Les profils d'application définissent l'utilisation de certaines

options des normes de base et fournissent une base pour l'échange de données entre applications et l'interopérabilité des systèmes.

4.1.2. Biométrie

Relevant du domaine de la biométrie, utilisé comme adjectif.

Note (pour l'anglais): «biometric» ne doit plus être utilisé comme substantif.

4.1.3. Authentification biométrique/authentifier biométriquement

Authentifier l'identité d'un individu au moyen d'un système de vérification ou d'identification biométrique.

4.1.4. Bloc de données biométriques (BDB)

Bloc de données mémorisées sous un format prédéfini contenant un ou plusieurs échantillons ou gabarits biométriques.

4.1.5. Identification biométrique/identifier biométriquement

Comparer un échantillon biométrique à l'ensemble des échantillons traités et mémorisés dans la base de données biométriques afin de l'apparier à l'un d'entre eux et d'obtenir un indice de comparaison indiquant le degré de similitude des échantillons comparés.

4.1.6. Enregistrement d'informations biométriques

Structure de données contenant un bloc de données biométriques, des informations précisant le format sous lequel elles ont été enregistrées et, éventuellement, d'autres informations comme par exemple si le BDB est numériquement signé ou crypté.

4.1.7. Enregistrement de données biométriques d'échange

Ensemble de données, concernant une seule personne, contenant des informations biométriques (section 4.1.6) ainsi que d'autres informations concernant spécifiquement les systèmes, applications ou fonctions relatifs aux pièces d'identité des marins.

4.1.8. Echantillon biométrique

Données recueillies à l'aide d'un lecteur biométrique, enregistrées soit directement soit après traitement.

4.1.9. Vérification biométrique/vérifier biométriquement

Opération consistant à vérifier qu'un échantillon biométrique est semblable à l'échantillon biométrique précédemment traité et mémorisé correspondant à l'identité que prétend posséder l'intéressé, en appariant les gabarits pour obtenir un indice qui est ensuite comparé à un seuil de validation.

4.1.10. Enrôlement biométrique

Procédé consistant à recueillir un échantillon biométrique, ou plusieurs, auprès d'un individu et à traiter puis à mémoriser un ou plusieurs de ces échantillons ainsi que d'autres données relatives à l'identité de l'individu concerné.

4.1.11. Code des noms de pays

Codes numériques à trois chiffres spécifiés dans la norme ISO 3166-1.

4.1.12. Intégrité des données

Le système la garantit lorsque les données enregistrées sur un support physique, tel qu'une PIM ou une base de données électroniques nationale sur les PIM, ne peuvent être modifiées sans que cela ne soit décelé et sans que l'origine de l'altération ne puisse être détectée.

4.1.13. Confidentialité des données

Le système la garantit lorsque l'accès aux données enregistrées sur un support physique tel qu'une PIM ou une base de données électroniques nationale sur les PIM, ou le traitement de ces données, sont réservés à certaines personnes ou pour des applications expressément autorisées, dotées de la capacité technologique nécessaire.

4.1.14. Interopérabilité à l'échelle mondiale des données biométriques enregistrées sur les pièces d'identité des gens de mer

Acceptation à l'échelle mondiale du bloc de données biométriques relatives aux empreintes digitales mémorisé sur le code-barres bidimensionnel imprimé sur la PIM aux fins d'authentifier l'identité du marin.

4.1.15. Terminaison zéro

Finissant par un octet zéro (0 x 00).

4.1.16. Temps réel

Caractérise un mode opératoire informatique selon lequel l'ordinateur recueille des données, les traite et en utilise les résultats pour le contrôle instantané d'un procédé.

4.1.17. Secondes depuis l'époque

Secondes depuis l'époque, dans un entier non signé de 32 bits, de la journée spécifiée comme défini dans la norme ISO/IEC 9945-1:2003, section 4.14. Toute seconde d'une journée donnée est acceptable, mais, si elle n'est pas effectivement connue, l'application PIM se calera par défaut sur la première seconde de cette journée.

4.1.18. Utilisation du présent

Conformément à la pratique juridique, le présent indique une obligation.

4.1.19. Utilisation du conditionnel

Conformément à la pratique juridique, le conditionnel indique une recommandation.

4.1.20. Jeux de caractères graphiques

Jeux de caractères graphiques d'encodage conformes à la norme ISO 8859-15:1999 (alphabet latin).

5. Conditions que doit remplir le système biométrique permettant l'établissement des PIM

5.1. Conditions que doit remplir le système biométrique d'établissement des PIM à partir du dessin papillaire digital

Les gabarits biométriques des dessins papillaires de deux doigts du marin destinataire du document sont imprimés sous forme chiffrée dans un code-barres conforme à la norme énoncée dans le présent document. La convention n° 185 de l'OIT fixe un certain nombre de préconditions auxquelles doit répondre le système finalement sélectionné qui sont présentées ci-après, suivies d'un exposé de ce que leur respect présuppose selon les auteurs du rapport.

- «les données biométriques peuvent être recueillies sans aucune intrusion dans la vie privée des intéressés, sans désagrément pour eux, sans risque pour leur santé et sans atteinte à leur dignité;» (convention de l'OIT n° 185, article 3, paragraphe 8 a)).

On suppose que les marins ne percevront pas la saisie et la vérification de leurs empreintes comme une intrusion dans leur vie privée ou une offense à leur dignité. L'ergonomie des appareils de saisie des données biométriques et de lecture des codes-barres sera telle que le marin ne subira aucun désagrément. Les risques pour la santé des marins seront évalués tant au stade de la saisie initiale que des vérifications ultérieures et les appareils seront régulièrement aseptisés pour prévenir tout risque de propagation de microbes par contact avec leurs éléments de sorte que leur utilisation ne présente pas plus de danger pour la santé que le contact avec une poignée de porte par exemple.

- «les données biométriques sont visibles sur la pièce d'identité et ne peuvent être reproduites à partir du modèle ou d'autres représentations;» (convention de l'OIT n° 185, article 3, paragraphe 8 b)).

Il doit être suffisamment difficile de reconstituer une empreinte digitale en tant que telle (c'est-à-dire «une image d'empreinte digitale») ou de fabriquer un dispositif frauduleux pouvant être utilisé pour dénaturer l'intention ou falsifier la présence du marin à partir des données biométriques enregistrées dans le code-barres. Les données biométriques des empreintes digitales sont par ailleurs considérées comme étant visibles lorsque le code-barres dans lequel elles sont enregistrées est imprimé sur la génération suivante de PIM et on suppose aussi que le système faisant appel à l'utilisation de gabarits d'empreintes digitales que pourrait choisir l'OIT ne permettra pas l'utilisation, par d'éventuels imposteurs, des données biométriques enregistrées.

- «le matériel nécessaire au recueil et à la vérification des données biométriques est facile à utiliser et est généralement accessible aux gouvernements à faible coût;» (convention de l'OIT n° 185, article 3, paragraphe 8 c)).

On suppose ici que la bonne ergonomie des équipements biométriques en garantira la facilité d'utilisation pour ceux qui sont chargés de la mise en œuvre des systèmes et les utilisateurs. On suppose par ailleurs que le choix qu'a fait l'OIT d'un mode de stockage dans un code-barres des données biométriques relatives aux empreintes digitales, qui nécessite l'emploi de dispositifs de saisie de faible résolution moins coûteux, satisfait à la demande d'un système «généralement accessible aux gouvernements à faible coût».

- «le matériel nécessaire à la vérification des données biométriques peut être utilisé de manière commode et fiable dans les ports et dans les autres lieux, y compris les navires, où les autorités compétentes effectuent normalement le contrôle de l'identité;» (convention de l'OIT n° 185, article 3, paragraphe 8 d)).

On suppose que les systèmes d'enregistrement des données biométriques et les lecteurs de cartes pourront être utilisés de manière fiable à bord des navires, dans les ports et autres lieux sans être indûment sensibles à la salinité corrosive de l'air marin ambiant.

- «le système, y compris les matériels, les technologies et les procédures, dans lequel les données biométriques sont utilisées permet d'obtenir des résultats uniformes et fiables en matière d'authentification d'identité.» (convention de l'OIT n° 185, article 3, paragraphe 8 e))

Par résultats «uniformes», on entend que le système biométrique est conforme aux prescriptions du présent rapport technique pour répondre à l'exigence d'interopérabilité. On suppose également que les systèmes biométriques commerciaux permettront une «authentification de l'identité» (au sens de «vérification de l'identité») fiable de l'ensemble des marins utilisant ces systèmes.

5.1.1 Procédure d'enrôlement biométrique

L'ensemble de la procédure de vérification d'identité que permet la PIM de l'OIT ne sera pas traité dans le présent rapport qui portera essentiellement sur la partie de la procédure relative à l'enrôlement biométrique. Une personne qualifiée chargée de délivrer le document enregistrera dans le système d'enrôlement les informations personnelles dont la liste est donnée à l'annexe A. Une empreinte digitale de l'index de chaque main devrait être saisie². Si l'empreinte de l'index n'existe plus ou est endommagée, au point que soit l'on ne peut pas saisir une empreinte fiable, soit on ne peut pas l'enrôler en raison de sa mauvaise qualité, on saisira alors l'empreinte d'un autre doigt ou d'un pouce en veillant à ce que la cohérence et l'efficacité opérationnelles soient maximales sans causer de désagrément au marin. L'ordre de présentation standard des doigts aux fins de l'enrôlement est le suivant:

- index de la main droite;
- index de la main gauche;
- pouce de la main droite;
- pouce de la main gauche;
- majeur de la main droite;
- majeur de la main gauche;
- annulaire de la main droite;

² La saisie de l'empreinte de deux doigts permet d'améliorer la fiabilité et la solidité du système. L'index est choisi en priorité car, dans la plupart des cas, c'est le doigt que l'on peut placer le plus facilement sur l'appareil de saisie, ce qui garantit au marin le minimum d'inconfort (convention, article 3, paragraphe 8, première condition préalable).

- annulaire de la main gauche;
- auriculaire de la main droite;
- auriculaire de la main gauche.

La personne chargée de délivrer les PIM précisera au moment de l'enrôlement quel est le doigt dont l'empreinte a été saisie et enregistrera cette information dans l'en-tête du gabarit biométrique mémorisé dans le code-barres de la PIM (voir annexe B).

Le système doit soit être doté d'un moyen de mesure automatique de la qualité de la saisie, soit fournir à la personne effectuant l'enrôlement le moyen d'évaluer celle-ci grâce à la signalisation d'un seuil d'acceptabilité permettant de garantir la création de gabarits de bonne qualité. Des empreintes de la meilleure qualité possible devraient être enrôlées et les gabarits d'empreintes digitales devraient être mémorisés de façon à permettre des vérifications fiables. Le marin pourra vérifier que les données biométriques de référence mémorisées sur sa PIM peuvent permettre d'effectuer une vérification biométrique, en particulier sur le lieu de délivrance de son document.

Le système biométrique de saisie d'empreintes digitales doit:

- afficher des messages sur écran lors de la procédure d'enrôlement, adressés à la fois à la personne chargée de délivrer la PIM et au marin, indiquant notamment la marche à suivre, la qualité de la saisie et la manière de positionner le doigt;
- permettre de connaître la teneur et la qualité des gabarits saisis et de les évaluer par rapport à des seuils fixés à l'avance de telle sorte que, si nécessaire, le marin puisse être invité à présenter soit le même doigt pour le réenrôler, soit le doigt suivant;
- donner une indication de la qualité du gabarit d'empreinte digitale saisi et renvoyer à l'opérateur (c'est-à-dire la personne délivrant la PIM) ainsi qu'à la personne enrôlée (c'est-à-dire le marin) une image de l'empreinte digitale enregistrée;
- permettre à la personne chargée de délivrer la PIM de choisir un autre doigt aux fins d'enrôlement si le système ne réussit pas à enregistrer un gabarit d'une qualité acceptable pour un doigt donné;
- permettre au marin de vérifier biométriquement avant l'impression du code-barres sur sa PIM si le gabarit saisi correspond à l'empreinte digitale enrôlée et lui est acceptable au plan opérationnel; une indication positive doit être donnée (identité vérifiée) si la valeur d'appariement est supérieure au seuil fixé aux fins de vérification (voir 5.3.1 ci-après) et une indication négative (identité non vérifiée) si le seuil d'appariement est en deçà du seuil de correspondance;
- fournir une indication du nombre de doigts correctement enrôlés;
- permettre à la personne délivrant la PIM de revoir les données textuelles saisies, de les modifier si nécessaire et d'imprimer le code-barres sur la PIM.
- permettre la vérification biométrique de l'identité du marin à l'aide de la PIM imprimée comme indiqué à la section 5.3.1.

5.1.2. Documentation relative à l'enrôlement biométrique

Une documentation facile à consulter doit être fournie afin que la personne chargée d'effectuer l'enrôlement sache comment procéder pour garantir l'enrôlement d'empreintes digitales de bonne qualité et l'enregistrement de gabarits de bonne qualité sur les PIM.

5.1.3. Saisie des empreintes digitales

Lors de l'enrôlement et de la vérification, l'appareil de saisie permettra de recueillir des gabarits biométriques d'empreintes digitales conformes aux indications données au tableau 1 de l'annexe A de la norme ISO/IEC WD 19794-4 – Formats d'échange de données biométriques – Partie 4: Format d'échange de données relatives à des images digitales (ISO/IEC JTC 1 SC37 N 341, du 7 octobre 2003)³ (voir annexe D au présent document pour l'ensemble du projet de norme) avec au minimum un niveau 3⁴ de qualité de saisie des données d'empreinte comme indiqué ci-après.

- résolution du balayage: 98 pixels par cm (250 pixels par pouce);
- nombre de bits par pixel: 3;
- gamme dynamique (niveaux de gris): 8;
- certification: aucune.

Le dispositif de saisie des empreintes doit permettre de produire une image de 12,7 mm sur 12,7 mm (½ pouce sur ½ pouce) de l'empreinte digitale qui sera focalisée, de préférence, sur la partie centrale de l'empreinte.

Lorsque les données relatives à l'image de l'empreinte digitale sont transmises à l'algorithme d'extraction du gabarit, par exemple de l'appareil de saisie vers un ordinateur, elles doivent soit ne pas être comprimées, soit être comprimées de telle sorte qu'il n'y ait aucune perte de qualité.

5.1.4. Gabarit d'empreinte digitale

L'algorithme extraira un gabarit à partir de l'image de l'empreinte digitale saisie conformément à la norme ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 3: Données relatives aux empreintes digitales (ISO/IEC JTC 1 SC37 N 313, du 3 octobre 2003). Ce gabarit sera stocké dans la base de données électronique nationale de l'Etat Membre (base de données de la convention) et dans le code-barres bidimensionnel PDF417 figurant sur la PIM lors de la procédure d'enrôlement et sera utilisé à des fins de comparaison lors du processus de vérification.

Un gabarit d'empreinte digitale doit être mémorisé pour les raisons suivantes:

³ Il s'agit là d'un projet de norme en cours de révision dans le cadre du groupe de travail 3 d'ISO/IEC JTC 1 SC37. Nous pensons que les paramètres de qualité du niveau 3 resteront les mêmes lorsque le projet de norme sera finalement approuvé. Toutefois, les paramètres indiqués dans le présent document seront ceux qui primeront pour les PIM.

⁴ Une qualité de niveau 3 pour la saisie des empreintes digitales est acceptable pour des images devant être utilisées pour créer des gabarits d'empreintes digitales intégrales. Il est à noter que la qualité de la saisie des données relatives aux empreintes digitales est différente de la qualité de l'image imprimée à partir du code-barres figurant sur la PIM.

1. Les gabarits des empreintes de deux doigts du marin doivent être mémorisés dans le code-barres PDF417 figurant sur la PIM.
 - a) Le volume de mémoire informatique nécessaire pour stocker l'*image* des empreintes digitales de deux doigts, cryptée ou non, est supérieur à la capacité d'enregistrement du code-barres bidimensionnel PDF417 figurant sur la PIM.
 - b) La taille des gabarits créés à partir des minuties du doigt varie en fonction du nombre des minuties qui y sont détectées⁵. D'après la réponse à une demande d'informations adressée par l'OIT aux vendeurs d'équipement biométrique en décembre 2003, un gabarit de minuties type en contient entre 50 et 60. Toutefois, le nombre maximal de minuties pouvant être mémorisées dans le code-barres PDF417 de la PIM est limité à 96, soit 48 par doigt. Par conséquent, pour pouvoir enregistrer les gabarits de minuties de deux doigts sur le code-barres de la PIM, le nombre de minuties autorisé et le volume global des données à mémoriser doivent être limités. Deux solutions ont été envisagées à cet effet. La première consisterait à préciser le nombre maximal de minuties devant être stockées par empreinte digitale ainsi que la méthode préconisée par l'OIT pour établir l'ordre de priorité des minuties devant figurer dans le gabarit des PIM. La seconde solution serait de n'indiquer que le nombre maximal de minuties devant être mémorisées dans le code-barres PDF417 de la PIM de l'OIT. Or ni l'une ni l'autre de ces solutions n'a été jugée valable pour les raisons suivantes.
 - i) Dans leurs réponses à la demande que leur avait adressée le BIT en décembre 2003, les vendeurs d'appareils biométriques ont fait savoir qu'il n'existe pas de méthode systématisée de troncature des gabarits. Par conséquent, les effets sur la performance des systèmes biométriques individuels, s'ils devaient se conformer à une méthode de troncature donnée, ne peuvent être ni prévus ni garantis tant qu'un laboratoire qualifié n'a pas effectué des essais approfondis au préalable.
 - ii) D'autre part, si un vendeur opère une troncature de ses gabarits⁶ afin de rester dans les limites fixées pour le code-barres PDF417 de la PIM de l'OIT, les effets sur la performance des systèmes des autres fournisseurs ne peuvent être ni prévus ni garantis tant qu'un laboratoire qualifié n'a pas au préalable effectué des essais approfondis.
 - iii) Il serait utile de procéder à des essais pour évaluer les conséquences que pourrait avoir une limitation de la taille des gabarits ou l'imposition d'une méthode précise de hiérarchisation des minuties devant être incluses ou exclues avant l'adoption de l'une ou l'autre solution, mais le calendrier de l'OIT n'a pas permis la réalisation de tels essais techniques avant la publication du présent rapport.
 - c) Les gabarits établis à partir des dessins papillaires digitaux sont de taille fixe et les empreintes de deux doigts peuvent être enregistrées dans les limites de la mémoire du code-barres PDF417 de la PIM, conformément à la norme ISO/IEC

⁵ ISO/IEC CD 19794-2 – Format d'échange des données biométriques – Partie 2: Données relatives aux minuties digitales (ISO/IEC JTC 1 SC37 N 340, du 7 octobre 2003).

⁶ Une proposition pour la normalisation de la troncature des gabarits de minuties a récemment été soumise à l'ISO mais il n'apparaît pas clairement que des produits conformes à cette méthode soient disponibles, et le calendrier de l'OIT n'a pas permis de procéder à des essais techniques avant la publication de ce rapport.

WD 19794-3 – Formats d'échange de données biométriques – Partie 3: Données relatives aux dessins papillaires digitaux (ISO/IEC JTC 1 SC37 N 313, du 3 octobre 2003). (Ce document a été mis au point sous forme d'une norme intitulée ANSI/INCITS 377 – Format d'échange de données relatives aux dessins papillaires digitaux.) L'utilisation de gabarits d'empreintes digitales de taille fixe a été testée dans les règles.

2. Conformément aux prescriptions de la convention n° 185, les gouvernements doivent en règle générale pouvoir se procurer des systèmes homologués pour un faible coût.
 - a) Conformément à la norme ISO/IEC WD 19794-4 – Formats d'échange des données biométriques – Partie 4: Format d'échange de données relatives aux images digitales (ISO/IEC JTC 1 SC37 N 341, du 7 octobre 2003), le degré de résolution des images nécessaires pour appliquer des algorithmes d'extraction dans le cas de dessins papillaires digitaux est inférieur à celui requis pour des minuties (250 pixels par pouce au lieu de 500 pixels par pouce). Donc, si l'on applique des algorithmes à des dessins papillaires digitaux, on peut utiliser des dispositifs de saisie moins onéreux offrant une résolution de 250 pixels par pouce.
3. D'après la convention n° 185, il ne doit pas être possible de reconstituer les données biométriques à partir du gabarit ni de toute autre représentation.
 - a) Les données biométriques stockées sur la PIM ne doivent pas permettre une utilisation frauduleuse des gabarits biométriques des marins; il doit être en particulier suffisamment difficile de reconstituer à partir des données biométriques enregistrées dans le code-barres une empreinte digitale en tant que telle (c'est-à-dire une «image de l'empreinte digitale») ou de mettre au point un dispositif frauduleux permettant de reconstituer une fausse empreinte digitale du marin.
 - b) Il peut être possible de reconstituer l'image d'une empreinte digitale ou de mettre au point un dispositif frauduleux permettant d'obtenir une fausse empreinte du marin à partir des données enregistrées dans des gabarits de minuties et d'images d'empreintes digitales⁷. Toutefois, aucune publication ne fait état d'une méthode permettant, à partir des données enregistrées dans des gabarits établis à partir de dessins papillaires digitaux, de reconstituer l'image d'une empreinte ou de mettre au point un dispositif frauduleux permettant de falsifier l'empreinte du marin⁸.

Le gabarit biométrique établi à partir des dessins papillaires digitaux devant figurer sur les PIM de l'OIT est spécifié dans les annexes A, B et C et obéit à la norme ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 3: Données relatives aux dessins papillaires digitaux (ISO/IEC JTC 1 SC37 N 313, du 3 octobre 2003). La structure des données mémorisées dans le code-barres de la pièce d'identité des marins est en résumé la suivante:

- En-tête conforme à la norme BioAPI – 16 octets.

⁷ Bromba, M.: «On the reconstruction of biometric raw data from template data», 9 juillet 2003. Peut être téléchargé à partir du site: <http://www.bromba.com/knowhow/temppriv.htm>.

⁸ Hill, C.J.; Risk of Masquerade Arising from the Storage of Biometrics, B.S. Thèse, Australian National University, 2001. Peut être téléchargé à partir du site: <http://chris.fornax.net/biometrics.html>.

- En-tête contenant les données relatives aux empreintes digitales – 32 octets.
- Gabarits de deux empreintes digitales – 520 octets.
- Chaque gabarit d’empreinte digitale comportera 224 cellules: 14 cellules par rangée, sur 16 rangées. Chaque cellule aura une profondeur d’angle de 3 bits, une profondeur de longueur d’onde de 3 bits, et une profondeur de décalage de phase de 3 bits.
- Représentation numérique des données décrite à l’annexe A – 120 octets.
- Nombre total d’octets dans le code-barres figurant sur la PIM – 688.

5.2. Prescriptions relatives au code-barres utilisé sur les PIM

5.2.1. Format du code-barres

Le code-barres utilisé sur la PIM sera formaté conformément à l’annexe A. Pour les empreintes digitales créées à partir des minuties, il contiendra au maximum 686 octets, auxquels s’ajouteront 64 symboles de données pour un niveau 5 de correction d’erreur. Il comprendra les données du gabarit biométrique ainsi que les informations à imprimer au recto de la PIM, à savoir: l’autorité de délivrance, le numéro d’identification personnel (facultatif), le nom en entier du marin, le numéro unique du document, la date d’expiration du document, la nationalité du marin, la date et le lieu de naissance, le sexe ainsi que le lieu et la date de délivrance du document (voir l’annexe A). Les gabarits biométriques des empreintes de deux doigts du marin seront formatés conformément à l’annexe B, qui définit le bloc de données biométriques de 568 octets au maximum, visé à l’annexe A. Ce bloc de données biométriques de 568 octets au maximum plus l’information d’en-tête de 120 octets définie à l’annexe A composent le code-barres de la PIM, dont le contenu total représente donc 688 octets.

La technologie du code-barres bidimensionnel PDF417 2-D s’appliquera pour les raisons suivantes:

- les symboles PDF417 répondent aux prescriptions relatives à la capacité de stockage de données requise pour cette application;
- les symboles PDF417 peuvent se lire à l’aide d’un scanner bidimensionnel ou d’un lecteur optique standard – CCD ou à laser – et d’un logiciel spécial de décodage. Toutefois, les crayons lecteurs ne pourront pas lire ces symboles. Cette vaste gamme de lecteurs optiques des codes-barres à usage commercial, qui sont d’un prix abordable, facilitera la vérification par la biométrie de l’identité des membres de la communauté des gens de mer.

Les dimensions et l’emplacement du code-barres seront conformes aux spécifications de l’Organisation de l’aviation civile internationale (OACI), telles qu’elles figurent dans son document 9303, Partie 1 (5^e édition, 2003) et Partie 3 (2^e édition, 2002), et telles qu’elles sont mentionnées ci-après pour la commodité du lecteur:

- pour les livrets PIM, la taille maximale du code-barres est de 21,35 mm x 86 mm, zones non imprimées comprises, ainsi que spécifié par l’OACI dans le document 9303, Partie 1 – Passeports lisibles à la machine – IV Spécifications techniques particulières aux passeports lisibles à la machine – Annexe E (normative) – Utilisation de code(s)-barres sur la page de données des passeports lisibles à la machine (MRP);

- pour les cartes PIM, la taille maximale du code-barres est de 27,8 mm x 85,6 mm⁹, zones non imprimées comprises (voir le document 9303 de l'OACI, Partie 3 – Les documents de voyage officiels lisibles à la machine de formats 1 et 2 –, Annexe E (normative) à la section IV – Utilisation du/des code(s)-barres optionnels sur le TD-1).

En outre, le code-barres utilisé sur la PIM sera conforme aux spécifications suivantes:

- dimension X: la largeur du module de symboles est comprise entre une valeur minimale de 0,170 mm (plus grande pour remplir, si possible, la zone de carte) et une valeur maximale de 0,175 mm;
- dimension Y: la hauteur de rangée est comprise entre une valeur minimale de 0,511 mm (trois fois la dimension X, voire plus grande pour remplir, si possible, la zone de carte) et une valeur maximale de 0,525 mm;
- un niveau 5 de correction d'erreur, comme recommandé dans les normes ISO/IEC 15438:2001, Annexe E, et dans le document 9303 de l'OACI – Partie 3 (2^e édition, 2002);
- 16 colonnes pour les symboles de données¹⁰;
- le nombre de rangées requises (40) pour y faire figurer les données¹¹.

5.2.2. La technologie des imprimantes et les spécifications relatives à l'impression

Le code-barres PDF417 sera imprimé sur la PIM conformément à la norme ISO/IEC 15438:2001. Il est possible d'imprimer les symboles PDF417 du code-barres bidimensionnel avec la plupart des imprimantes de marque de la gamme professionnelle, à transfert thermique, à laser et à jet d'encre. La qualité d'impression du code-barres sur la PIM de prochaine génération sera conforme au projet de norme ISO/IEC FDIS 15415 – Spécification relative au contrôle de la qualité d'impression du code-barres – Deux

⁹ Cela signifie que la PIM de prochaine génération, qui se présentera sous forme de carte, sera un document de voyage lisible à la machine (MRTD) de format 1 et non pas 2, ainsi que spécifié par le document 9303 de l'OACI – Partie 3 (2^e édition, 2002).

¹⁰ Selon les termes de M. Sprague Ackley, expert internationalement reconnu en technologie des codes-barres bidimensionnels PDF417 2-D: « S'il est difficile d'établir avec certitude à partir de quand les systèmes d'imagerie bidimensionnelle commencent à avoir des problèmes avec les symboles PDF 417 dans de nombreuses colonnes, il est quasiment assuré, en revanche, que 25 colonnes de données mettront à mal plusieurs de ces systèmes d'imagerie ». L'utilisation de 16 colonnes de données (20 au total) permettra d'appliquer la technologie de lecture de codes-barres du type scanner bidimensionnel, laissant suffisamment d'espace dans le sens vertical pour intégrer sur la PIM le code-barres et d'autres données.

¹¹ Ci-après est déterminé par dérivation le nombre de rangées requises dans le format du code-barres utilisé sur la PIM pour les empreintes digitales réduites aux minuties. Les données de la PIM représentent 686 octets. Chaque mot de code peut stocker 1,2 octet. Le nombre de mots de code est donc: $686/1,2 = 572$; 64 mots de code supplémentaires sont nécessaires pour les codes de correction d'erreur de niveau 5, plus un mot de code pour la taille totale du code-barres, ce qui fait au total: $572 + 64 + 1 = 637$ symboles de données sur le code-barres de la PIM. Il y a 16 colonnes de données. Par conséquent, $637/16 = 40$ rangées requises pour stocker les données du code-barres sur la PIM.

symboles bidimensionnels, avec la désignation 3.0/05/660. Cette désignation se réfère au niveau 3 de définition des symboles, obtenu avec une ouverture de 0,125 mm pour une longueur d'onde de 660 nanomètres.

Le code-barres de la PIM sera imprimé de telle manière que le document ainsi obtenu soit suffisamment résistant dans l'optique de son utilisation comme document d'identification de gens de mer.

La zone imprimable réservée au code-barres sera conforme aux spécifications de l'OACI telles qu'elles figurent dans le document 9303, Partie 1 (5^e édition, 2003) et Partie 3 (2^e édition, 2002).

5.2.3. La technologie des lecteurs

Les symboles PDF417 utilisés sur les PIM de prochaine génération seront lus à l'aide d'un scanner bidimensionnel ou d'un lecteur standard – CCD ou à laser – et d'un logiciel de décodage spécial capable de lire les codes-barres imprimés conformément aux paragraphes 5.2.1 et 5.2.2 ci-dessus. Cependant, les crayons lecteurs ne pourront pas lire les symboles PDF417.

5.2.4. Caractéristiques physiques des codes-barres

Le «modèle biométrique correspondant à une empreinte digitale traduite sous forme de chiffres dans un code-barres» (convention internationale du travail n° 185, annexe I, paragr. 3 k)) sera protégé «par un laminat ou une couche de laque, ou par l'application d'une technologie d'image ou d'un support matériel qui garantit une résistance équivalente à la substitution du portrait et d'autres données biographiques». (Convention internationale du travail n° 185, annexe I.) Cette protection améliorera également la durabilité du code-barres.

«Les données biométriques sont visibles sur la pièce d'identité.» (Convention internationale du travail n° 185, art. 3, paragr. 8 b.) Cette disposition signifie que les données biométriques sont réputées visibles lorsque le code-barres où sont stockées les données biométriques des empreintes digitales est imprimé sur la PIM de nouvelle génération. Le code-barres est visible s'il est imprimé sur la PIM. Par ailleurs, le marin devra avoir la possibilité de voir une représentation binaire du gabarit traduit en code-barres et de vérifier lui-même les données biométriques en utilisant la PIM comme source de données de référence là où se trouve une autorité délivrant des PIM.

5.3. **Prescriptions relatives à la vérification des données biométriques des PIM**

5.3.1. Procédure de vérification des données biométriques

Un lecteur balaisera le code-barres de la PIM et lira les informations d'en-tête et les données du gabarit. L'en-tête spécifiera les doigts dont les empreintes sont stockées dans le code-barres.

Le système demandera au marin de placer un premier doigt aux fins de lecture optique du gabarit digital traduit en code-barres.

Si le doigt correspondant au premier doigt enrôlé est manquant, endommagé, n'est pas saisi ou n'obtient pas, après trois essais, un score de correspondance supérieur à la valeur seuil, le système demandera au marin de placer le second doigt enrôlé sur le dispositif de capture biométrique. Si un doigt soumis au balayage direct (live scan) correspond aux gabarits stockés dans le code-barres, le marin aura passé le contrôle avec

succès. Si aucun des doigts soumis au balayage direct ne correspond aux gabarits stockés dans le code-barres, le système affichera un message d'échec de vérification. Si, après le troisième essai pour chacun des deux doigts enrôlés, le système affiche un message d'échec, aucune vérification supplémentaire ne sera effectuée avec la même PIM sans l'intervention du personnel autorisé.

Le système de reconnaissance biométrique des empreintes digitales devra:

- retrouver le gabarit à partir du code-barres bidimensionnel PDF417 figurant sur la PIM;
- afficher à l'écran des messages à l'intention de l'autorité de vérification des PIM et du marin pour mener à bien la session de vérification, des messages indiquant la procédure à suivre, des réactions concernant le placement des doigts ainsi que les résultats obtenus;
- demander au marin de placer le doigt approprié sur le capteur d'image;
- comparer l'image saisie des empreintes digitales avec le gabarit correspondant stocké dans le code-barres;
- donner un signal de concordance (identité confirmée) lorsque le score de correspondance est supérieur à la valeur seuil, et un signal de non-concordance (identité non confirmée) lorsque le score de correspondance est inférieur à cette valeur;
- exiger l'intervention du personnel de vérification lorsque, après trois essais par doigt, le marin ne satisfait au contrôle pour aucun des doigts enrôlés.

Le système de reconnaissance biométrique des empreintes digitales devrait:

- avoir un seuil de correspondance tel qu'aussi bien le taux de fausses acceptations que le taux de faux rejets pour le grand public soient inférieurs à 1 pour cent;
- avoir des mesures de contenu et de qualité proportionnelles aux mesures de qualité utilisées pour l'enrôlement;
- prévoir, à titre facultatif, une mesure indiquant la qualité d'enrôlement.

5.3.2. Documentation relative à la vérification des données biométriques

Une documentation conviviale sera fournie au personnel pour qu'il puisse s'initier aux modalités de la procédure de vérification.

5.4. Prescriptions relatives aux bases de données concernant les PIM

5.4.1. Base de données sur les codes-barres

«Les gens de mer disposeront d'un accès facile à des équipements leur permettant d'examiner toute donnée les concernant qui ne peut faire l'objet d'un examen visuel. Cet accès sera donné par l'autorité qui délivre la pièce d'identité ou en son nom.» (Convention internationale du travail n° 185, art. 3, paragr. 9.) Le «modèle biométrique» correspondra «à une empreinte digitale traduite sous forme de chiffres dans un code-barres répondant à une norme» [la présente norme] (convention internationale du travail n° 185, annexe I).

L'autorité qui délivre les PIM permettra aux gens de mer d'accéder aux machines afin de leur permettre d'inspecter les données stockées dans le code-barres bidimensionnel PDF417 utilisé sur la PIM. Le marin aura la possibilité de vérifier si les gabarits d'empreintes digitales stockés dans sa carte correspondent à ceux des doigts enrôlés. Les données autres que les empreintes digitales seront affichées en texte.

5.4.2. Base de données électronique nationale sur les PIM

La convention n° 185 de l'OIT comporte un ensemble de prescriptions auxquelles il convient de se conformer ainsi qu'un ensemble de prescriptions auxquelles chaque Membre devrait se conformer en ce qui concerne la base de données électronique nationale concernant les PIM, qui aura un impact sur la mise en œuvre et l'utilisation du système de reconnaissance biométrique. Ces prescriptions sont mises en exergue ci-après, avec la stratégie de conformité que les auteurs du profil biométrique en question sont censés appliquer.

- «Les renseignements à fournir pour chaque enregistrement dans la base de données électronique que tout Membre doit tenir à jour, conformément aux paragraphes 1, 2, 6 et 7 de l'article 4 de la présente convention [n° 185] [de la Conférence internationale du Travail] doivent se limiter aux éléments suivants:

1. autorité de délivrance indiquée sur la pièce d'identité;
2. nom en entier du marin tel qu'inscrit sur la pièce d'identité;
3. numéro unique du document;
4. date d'expiration, de suspension ou de retrait de la pièce d'identité;
5. modèle biométrique figurant sur la pièce d'identité;
6. photographie (si elle est stockée sous forme numérique);
7. précisions sur toutes les demandes de renseignements effectuées sur les pièces d'identité des gens de mer. (Convention internationale du travail n° 185, annexe II.)

La base de données électronique nationale contiendra les enregistrements des sept éléments énumérés ci-dessus pour chaque marin à qui une PIM a été délivrée.

- «Aux fins de la présente convention, des restrictions appropriées sont établies afin d'assurer que des données, en particulier photographiques, ne puissent être échangées à moins qu'un mécanisme soit mis en place pour assurer que les normes applicables de protection des données et de la vie privée soient respectées.» (Convention internationale du travail n° 185, art. 4, paragr. 6.)

Des mécanismes de contrôle de l'accès à la base de données seront mis en place afin de protéger les informations concernant les marins de tout accès par des personnes non autorisées ou à des fins détournées.

- «Les renseignements correspondant à chaque point de l'annexe II [de la convention internationale du travail n° 185] sont [seront] saisis dans la base des données au moment où est délivrée la PIM.» (Convention internationale du travail n° 185, annexe III, Partie A, paragr. 3 b) i.)

Les bases de données électroniques nationales des Membres seront actualisées en temps utile chaque fois qu'une PIM est délivrée.

- «Chaque Membre fera en sorte qu'un enregistrement de chaque pièce d'identité des gens de mer, délivrée, suspendue ou retirée par lui, soit conservé dans une base de données électronique. Les mesures nécessaires sont prises pour protéger cette base de données contre toute intervention ou tout accès non autorisé.» (Convention internationale du travail n° 185, art. 4, paragr. 1.) «La pièce d'identité des gens de mer est rapidement retirée par l'Etat qui l'a délivrée s'il est avéré que le marin ne répond plus aux conditions de délivrance fixées par la présente convention.» (Convention internationale du travail n° 185, art. 7, paragr. 2.) «L'autorité qui délivre les PIM devrait établir des procédures appropriées pour protéger la base de données, notamment: permission aux seuls fonctionnaires spécialement autorisés d'avoir accès à une entrée saisie dans la base de données ou d'y apporter un changement une fois que cette entrée a été confirmée par le fonctionnaire qui l'a saisie.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 4.2.2.)

Les bases de données électroniques nationales des Membres assureront une fonction de contrôle de gestion consistant à consigner les transactions, notamment la délivrance, la suspension ou le retrait/annulation de PIM. Des mécanismes de contrôle de l'accès à la base de données seront mis en place afin de protéger les informations concernant le marin de tout accès par des personnes non autorisées ou à des fins détournées. Les fonctionnaires spécialement autorisés de chaque organisation du Membre pourront, dans certaines limites, apporter des changements au journal de vérification; le Membre tiendra à jour les documents attestant ces changements.

- «Lorsqu'une PIM est suspendue ou retirée, des mesures doivent [devront] être prises rapidement pour actualiser la base de données.» (Convention internationale du travail n° 185, annexe III, Partie A, paragr. 3 c)).

Les bases de données électroniques nationales des Etats Membres seront actualisées en temps utile chaque fois qu'une PIM est suspendue ou retirée.

- «Un système de prolongation ou de renouvellement est [sera] mis en place pour répondre aux situations où le marin a besoin d'une prolongation ou d'un renouvellement de sa PIM ou aux situations de perte de PIM.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.) Le requérant ne devrait pas recevoir de PIM s'il en possède déjà une.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.)

Les Membres mettront en place un système de prolongation et/ou de renouvellement pour répondre aux situations où le marin a besoin d'une prolongation ou d'un renouvellement de sa PIM ou aux solutions de perte de PIM. La prolongation et/ou le renouvellement de la PIM donnera lieu, en temps utile, à une transaction dans la base de données électronique nationale. Si une PIM est rejetée pour cause d'expiration, la base de données électronique nationale fera l'objet d'une vérification tendant à établir si la PIM a été prolongée ou renouvelée. Les gens de mer ne devraient posséder qu'une seule PIM à la fois. La délivrance d'une nouvelle PIM devrait invalider toute PIM que le marin aura reçu antérieurement. Le système de reconnaissance biométrique confirmera si la PIM a été à nouveau enregistrée/délivrée.

- «Un système de renouvellement prématuré devrait s'appliquer lorsqu'un marin sait à l'avance que, compte tenu de la période de son service, il ne sera pas en mesure de présenter sa demande de renouvellement à la date d'expiration.» (Convention

internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.1.) «Le requérant ne devrait pas recevoir de PIM s'il en possède déjà une.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.)

Les Membres mettront en place un système de prolongation et/ou de renouvellement pour répondre aux situations où le marin a besoin d'une prolongation ou d'un renouvellement de sa PIM ou aux situations de perte de PIM. Le marin pourra demander une prolongation et/ou un renouvellement à sa convenance dans la mesure où il sait qu'il ne sera pas en mesure de présenter sa demande de renouvellement à la date d'expiration. La prolongation et/ou le renouvellement de la PIM donnera lieu, en temps utile, à une transaction dans la base de données électronique nationale. Si la PIM est rejetée pour cause d'expiration, la base de données électronique nationale fera l'objet d'une vérification tendant à établir si la PIM a été prolongée ou renouvelée. Les gens de mer ne peuvent posséder qu'une seule PIM à la fois. La délivrance d'une nouvelle PIM devrait invalider toute PIM délivrée antérieurement au marin. Le système de reconnaissance biométrique confirmera si la PIM a été à nouveau enregistrée/délivrée.

- «Un système de remplacement devrait s'appliquer dans les cas de perte de PIM. Un document temporaire approprié peut être délivré.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.3.) «Le requérant ne devrait pas recevoir de PIM s'il en possède déjà une.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.)

Les Membres mettront en place un système de remplacement pour répondre aux situations où un marin perd sa PIM. Le remplacement de la PIM donnera lieu à une transaction en temps réel dans la base de données électronique nationale. Les gens de mer ne devraient posséder qu'une seule PIM à la fois. La délivrance d'une nouvelle PIM devrait invalider toute PIM que le marin aura reçue antérieurement. Le système de reconnaissance biométrique confirmera si la PIM a été à nouveau enregistrée/délivrée. Le marin pourra demander le remplacement de la PIM par un document temporaire, à sa convenance. Ce document temporaire devra être restitué. La base de données électronique nationale sera actualisée en temps utile de manière à tenir compte des changements apportés. Seule sera autorisée à délivrer des documents temporaires l'autorité qui a délivré la PIM d'origine.

- «L'autorité qui délivre les PIM devrait établir des procédures appropriées pour protéger la base de données, notamment l'obligation de faire régulièrement des copies de la base, qui seront conservées sur des supports tenus en lieu sûr, hors des locaux de l'autorité qui délivre les PIM.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 4.2.2.)

L'autorité de délivrance de chaque Membre fera régulièrement des copies de la base de données électronique nationale, qui seront conservées sur des supports tenus en lieu sûr, hors des locaux de l'autorité qui délivre les PIM.

- «Les informations enregistrées concernant les problèmes de fiabilité ou de sécurité de la base de données électronique, y compris les demandes de renseignements adressées à la base», devraient être tenues à jour par l'autorité de délivrance de chaque Membre.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 5.6.5.)

Les bases de données électroniques nationales des Membres assureront une fonction de contrôle de gestion consistant à consigner les problèmes ayant des incidences sur la fiabilité ou la sécurité de la base de données (y compris les demandes de renseignements adressées à la base).

Annexe 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.

Annexe 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 19794-3¹² – 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 0x00000238010401010301nn0200000008 – 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.



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

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**

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

ISO copyright office Case postale 56 CH-1211 Geneva 20 Tel: +41 22 749 01 11 Fax: +41 22 749 09 47 E-mail copyright@iso.org Web www.iso.org as appropriate, of the Copyright Manager of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the draft has been prepared]

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents	Page
Foreword	v
Introduction.....	vi
1 Scope	1
2 Conformance.....	1
3 Normative references	1
4 Terms and definitions.....	1
4.1 Biometric	1
4.2 Biometric Algorithm.....	1
4.3 Biometric Data.....	2
4.4 Biometric Sample.....	2
4.5 Biometric System.....	2
4.6 Bit-Depth.....	2
4.7 Capture	2
4.8 Cell	2
4.9 Cell Structure	2
4.10 Cell Quality Group	2
4.11 Comparison	3
4.12 Crop	3
4.13 Dimension	3
4.14 Down-sample.....	3
4.15 Encryption	3
4.16 Enrollment	3
4.17 Finger Pattern.....	3
4.18 Finger Pattern Interchange Data.....	3
4.19 Maximal Spatial Frequency	3
4.20 Packed Data Format.....	3
4.21 Pad	4
4.22 Raw Fingerprint Image	4
4.23 Reference Template	4
4.24 Resolution	4
4.25 Template Size.....	4
5 Finger Pattern Interchange Data.....	5
5.1 Overview	5
5.2 Step 1) Reduction in resolution	5
5.3 Step 2) Cellular Representation	5
5.3.1 Cell Structure	5
5.4 Quality.....	7
6 Finger Pattern Data Record.....	8
6.1 Introduction.....	8
6.2 Record Header	9
6.2.1 Format Identifier.....	9
6.2.2 Version Number	9
6.2.3 Length of Record	9
6.2.4 Capture Device ID	9
6.2.5 Number of Finger Patterns in Record.....	9
6.2.6 Resolution of Finger Pattern in x-direction.....	9
6.2.7 Resolution of Finger Pattern in y-direction.....	9
6.2.8 Number of Cells in x-direction	9
6.2.9 Number of Cells in y-direction	9

6.2.10	Number of Pixels in Cells in x-direction	10
6.2.11	Number of Pixels in Cells in y-direction	10
6.2.12	Cellular x-offset	10
6.2.13	Cellular y-offset	10
6.2.14	Bit-depth of Cell Structure Angle	10
6.2.15	Bit-depth of Cell Structure Wavelength	10
6.2.16	Bit-depth of Cell Structure Phase Offset	10
6.2.17	Bit-depth of Cell Structure Quality	10
6.2.18	Cell Quality Granularity	10
6.2.19	Reserved Bytes	10
6.3	Single Finger Pattern Record Format	11
6.3.1	Finger Pattern Record Header	11
6.3.2	Finger Pattern Data	13
Annex A	(informative) - Finger Pattern Data Record Example	16
A.1	Reduction in Resolution	16
A.2	Cellular Representation	17
A.3	Cell Structure	17
A.4	Quality	18
A.5	Data Record	18

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) \equiv 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

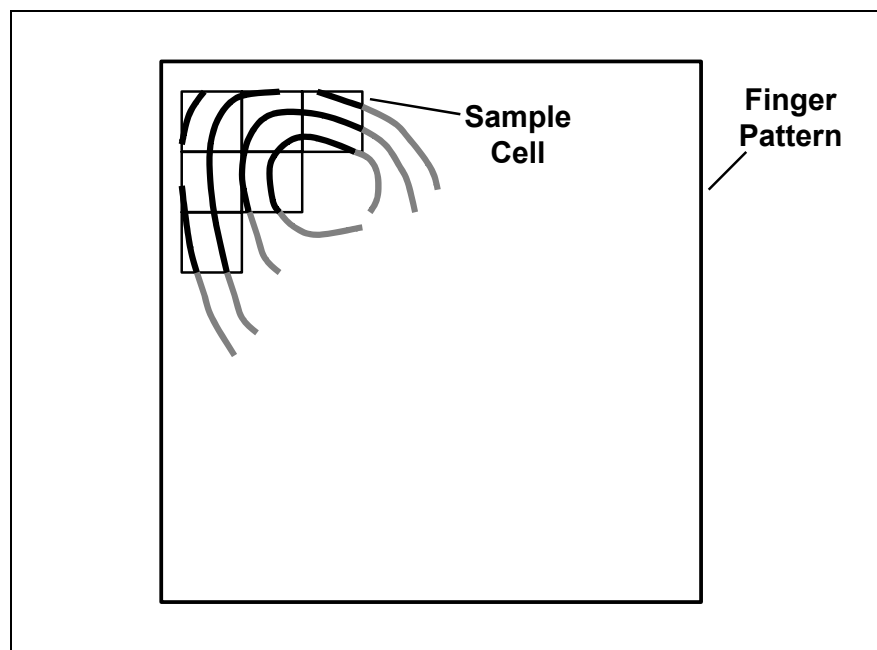


Figure 1. Diagram to illustrate Cellular Representation of Finger Pattern.

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).

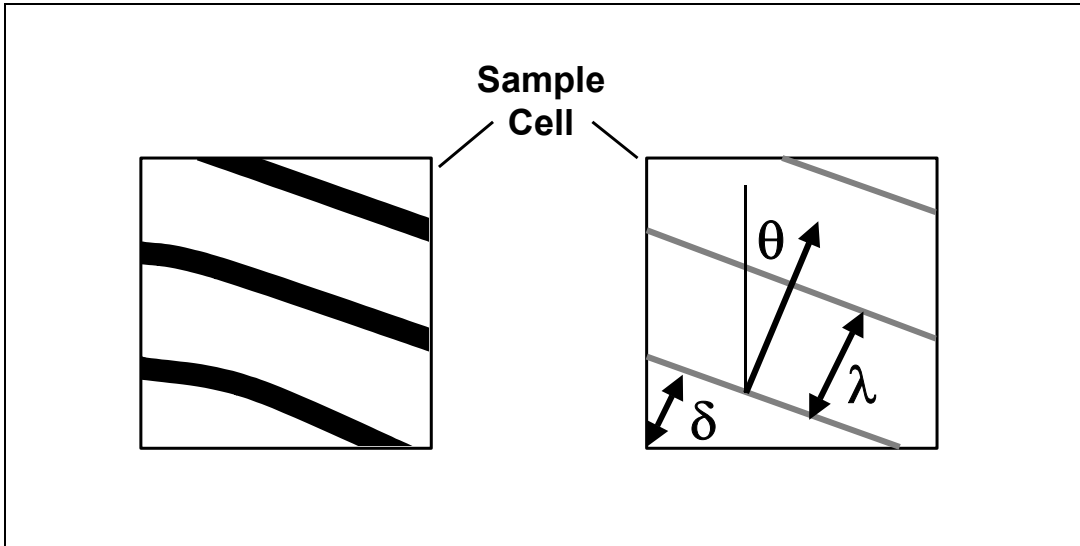


Figure 2. Cellular Representation of Finger Pattern.

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.

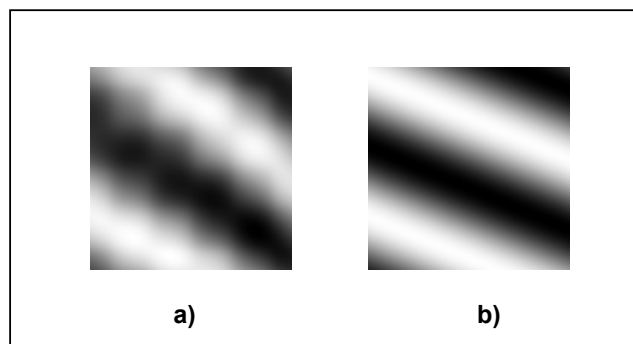


Figure 3. a) Example of the local finger pattern information in a cell, and b) the resulting cell structure chosen for representation.

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 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.

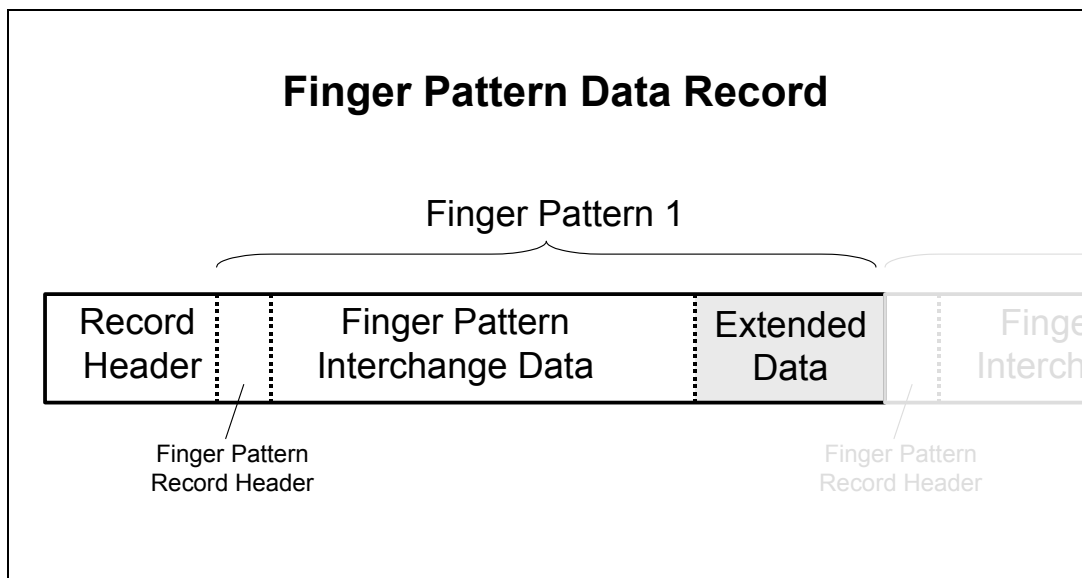


Figure 4. Diagram of Finger Pattern Data Record

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 $\text{SQRT}(\text{Number of Cells in Cell Quality Group})$.

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
<i>Plain right thumb</i>	<i>11</i>
<i>Plain left thumb</i>	<i>12</i>
<i>Plain right four</i>	<i>13</i>
<i>Plain left four fingers</i>	<i>14</i>

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.

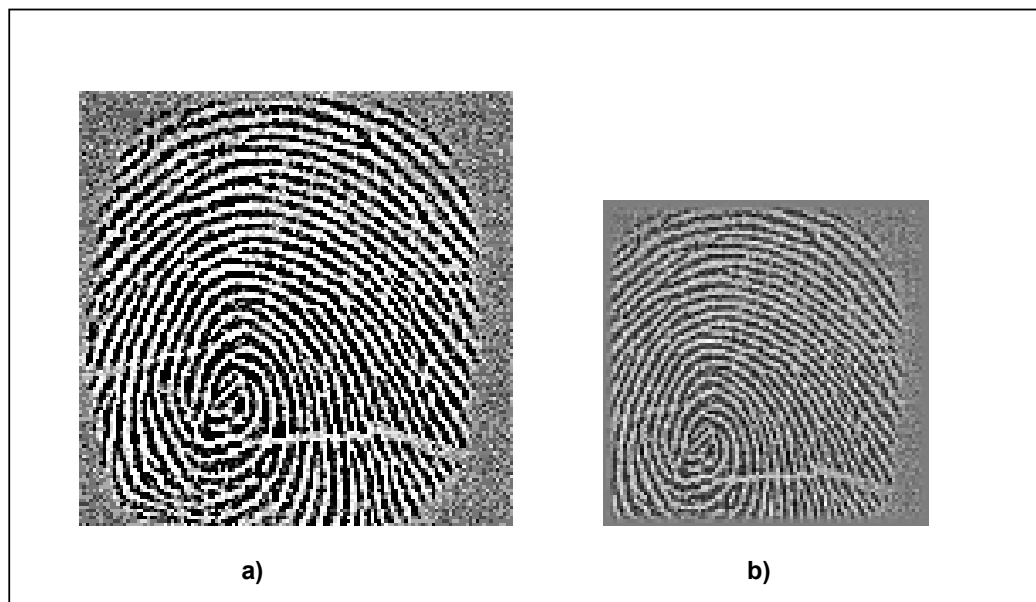


Figure 5. a) original 128x128 image sampled at 98.5 ppcm (250 ppi). b) resulting image after cropping image in a) to 120x120 pixels, and re-sampling image at 78.8 ppcm (200 ppi), to produce a 96x96 pixel dimensioned array.

A.2 Cellular Representation

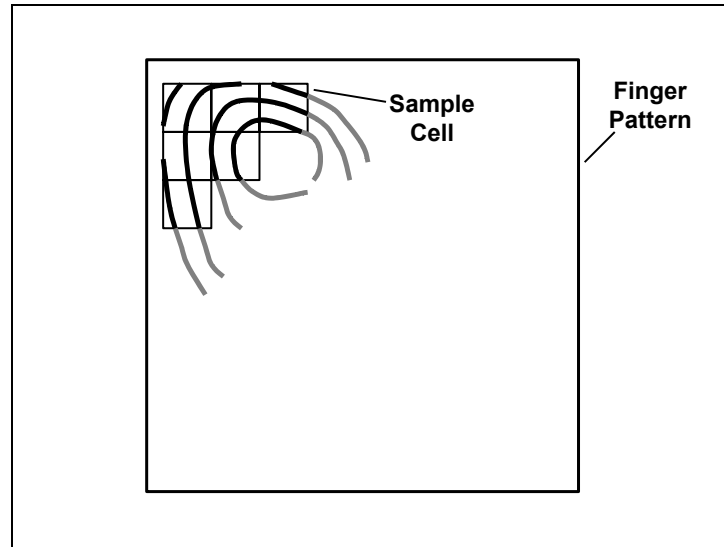


Figure 6. Diagram to illustrate Cellular Representation of Finger Pattern.

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).

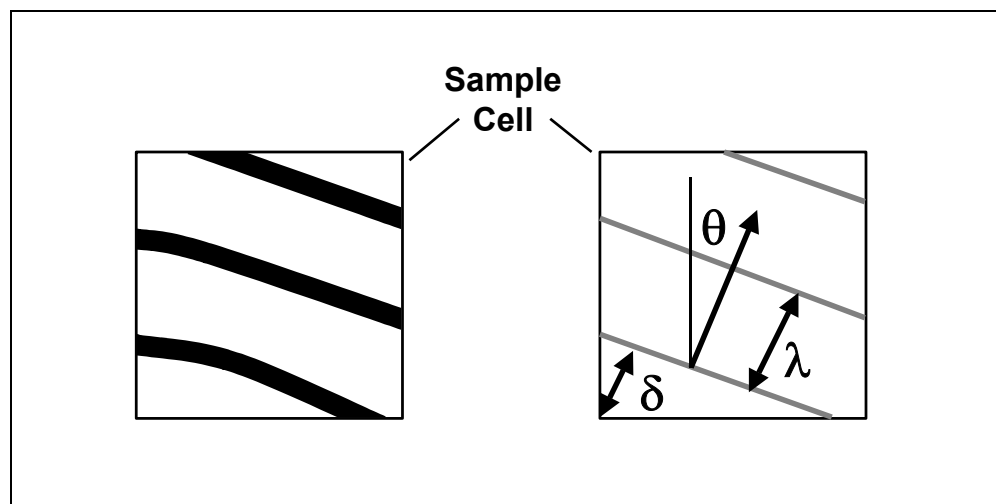


Figure 7. Cellular Representation of Finger Pattern.

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	



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

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) <p style="text-align: center;">2004-01-07</p> 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.

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

ISO copyright office
Case postale 56 CH-1211 Geneva 20
Tel: +41 22 749 01 11
Fax +41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

1	Scope	1
2	Conformance	1
3	Normative references	1
4	Terms and definitions	2
4.1	biometric sample	2
4.2	capture	2
4.3	core	2
4.4	fingerprint image area	2
4.5	friction ridge	2
4.6	grayscale	2
4.7	image resolution	2
4.8	live capture	2
4.9	pixel:	2
4.10	plain fingerprint image	2
4.11	ppcm	3
4.12	ppi	3
4.13	ppmm	3
4.14	rolled fingerprint image	3
4.15	scan resolution	3
4.16	transaction.....	3
4.17	valley.....	3
5	Data conventions	3
5.1	Byte and bit ordering	3
5.2	Scan sequence	3
6	Image requirements	4
6.1	Pixel aspect ratio	4
6.2	Pixel depth.....	4
6.3	Grayscale data	4
6.4	Dynamic range	4
6.5	Scan resolution	4
6.6	Image resolution	5
6.7	Fingerprint image location	5
7	Finger image record format.....	5
7.1	General record header	5
7.1.1	Format Identifier.....	6
7.1.2	Version number.....	6
7.1.3	Record length.....	6
7.1.4	Capture device ID.....	7
7.1.5	Number of finger/palm images.....	7
7.1.6	Scale units	7
7.1.7	Scan resolution (horizontal).....	7
7.1.8	Scan resolution (vertical)	7
7.1.9	Image resolution (horizontal).....	7
7.1.10	Image resolution (vertical)	7
7.1.11	Pixel depth.....	7
7.1.12	Image Compression algorithm.....	7
7.1.13	Reserved.....	8
7.2	Finger record header	8
7.2.1	Length of finger/palm data block.....	8

7.2.2	Finger/palm position	8
7.2.3	Count of views	9
7.2.4	View number.....	10
7.2.5	Finger/palm image quality	10
7.2.6	Impression type	10
7.2.7	Horizontal line length.....	10
7.2.8	Vertical line length	11
7.2.9	Finger/palm image data	11
Annex A	13
Annex B	14
Annex C	15

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*

ISO/IEC CD 19794-4

— *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 Standard 15444, 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 an 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 ppm

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 0-65535. 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 bytes		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 be 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		Height	
			(cm)	(in)	(cm)	(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: (1) 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:

$$D \leq 0.0007, \quad \text{for } 0 \leq X \leq 0.07$$

$$D \leq 0.01X, \quad \text{for } 0.07 \leq X \leq 1.50$$

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

The requirement corresponds to a positional accuracy of ∇ 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:

$$(\text{maximum} - \text{minimum}) / (\text{maximum} + \text{minimum})$$

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:

$$\text{MTF} = \text{representative image modulation} / \text{target modulation}$$

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

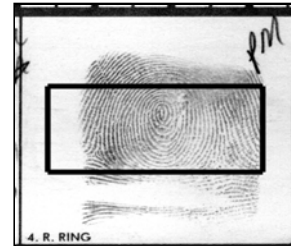
¹Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

²Sine 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, Munsell³ 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.

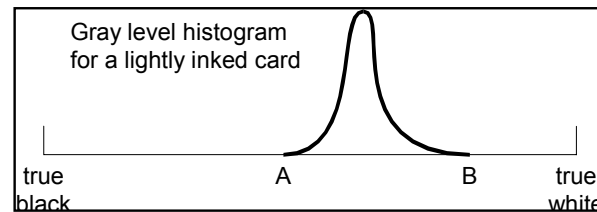
2.4 Gray-Scale Range of Image Data

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:

$$D \leq 0.0005, \quad \text{for } 0 \leq X \leq 0.07$$

$$D \leq 0.0071X, \quad \text{for } 0.07 \leq X \leq 1.50$$

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

The requirement corresponds to a positional accuracy of $\leq .71\%$ for distances between 0.07 and 1.5 inches, and a constant ≤ 0.0005 inches ($\frac{1}{2}$ 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:

⁴Applied 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:

$$(\text{maximum} - \text{minimum}) / (\text{maximum} + \text{minimum})$$

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:

$$\text{MTF} = \text{representative image modulation} / \text{target modulation}$$

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

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

Annexe II

Profil biométrique créé à partir des minuties digitales aux fins de l'établissement des pièces d'identité des gens de mer

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

Page

Table des matières

Avant-propos	2
0. Introduction	3
0.1. Principes de base de l'élaboration des documents.....	3
0.2. Travaux connexes	4
0.3. Détermination de l'option biométrique fondée sur les empreintes digitales	5
1. Champ d'application	5
2. Conformité	7
3. Références	7
3.1. Normes contraignantes.....	7
3.2. Documentation	8
3.3. Normes et documents complémentaires à élaborer ou à privilégier en vue d'une utilisation par les gens de mer.....	8
4. Définitions	8
4.1. Termes et définitions	8
5. Conditions que doit remplir le système biométrique permettant l'établissement des PIM	11
5.1. Conditions que doit remplir le système biométrique d'établissement des PIM à partir des minuties digitales	11
5.2. Prescriptions relatives au code-barres utilisé sur les PIM	16
5.3. Prescriptions relatives à la vérification des données biométriques des PIM	19
5.4. Prescriptions relatives aux bases de données concernant les PIM	20

Annexe A: SID minutiae-based fingerprint bar code format (normative)

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

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

Annexe D: ISO/IEC WD 19794-4 (ISO/IEC JTC 1 SC37 N 341, dated 7 October 2003)

Avant-propos

L'Organisation internationale du Travail, créée en 1919, est une institution spécialisée des Nations Unies. C'est un organisme tripartite, au sein duquel les représentants des gouvernements, des employeurs et des travailleurs sont placés sur un pied d'égalité. En juin 2003, l'OIT a adopté la convention n° 185 sur les pièces d'identité des gens de mer (révisée). La révision de la convention précédente, laquelle datait de 1958, a été motivée par les débats tenus au sein de l'Organisation maritime internationale (OMI) en vue d'examiner les mesures et règles propres à prévenir les actes de terrorisme qui menacent la sécurité des passagers et des équipages, ainsi que la sûreté des navires. La nouvelle convention de l'OIT a été communiquée aux gouvernements des Etats Membres de l'Organisation pour examen en vue de sa ratification. Elle aura un caractère obligatoire, au même titre qu'un traité international, pour tous les Membres qui l'ont ratifiée.

Le Bureau international du Travail, qui est le secrétariat de l'Organisation, a chargé les auteurs du présent document d'établir un projet de rapport technique qui constituera la base d'une norme à soumettre ultérieurement à l'ISO en vue d'obtenir son aval, cette norme portant sur un modèle biométrique interopérable conforme aux dispositions de la convention n° 185 et couvrant les domaines suivants: saisie des données relatives aux empreintes digitales, création de gabarits et stockage des codes-barres. Le rapport fera état des techniques et procédures les mieux adaptées dans les domaines suivants: imprimerie, lecture, enrôlement, format des codes-barres, détecteurs/lecteurs biométriques, considérations relatives aux bases de données et format d'un modèle biométrique interopérable au plan mondial. Le rapport devrait également prendre en considération les questions relatives aux bases de données concernant la qualité et l'interopérabilité.

L'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) constituent le système spécialisé de la normalisation mondiale. Les organes nationaux qui sont membres de l'ISO et de la CEI participent à l'élaboration des normes internationales dans le cadre des comités techniques créés par l'organisation compétente pour traiter des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent à des questions d'intérêt mutuel. D'autres organisations internationales, tant gouvernementales que non gouvernementales, participent également à ces travaux, en liaison avec l'ISO et la CEI.

Les normes internationales sont rédigées selon les règles énoncées à la partie 2 des directives de l'ISO et de la CEI.

Dans le domaine de l'informatique, l'ISO et la CEI ont créé un comité technique conjoint, qui transmet pour approbation aux organes nationaux les projets de normes internationales qu'il a adoptés.

Le présent rapport (ILO SID-0002), intitulé *Profil biométrique créé à partir des minuties digitales aux fins de l'établissement des pièces d'identité des gens de mer*, a été élaboré par le Bureau international du Travail. Il peut être soumis en tant que contribution technique au comité conjoint ISO/IEC JTC 1 SC37, *Biométrie*. Il se divise en cinq sections, à savoir:

- section 1 – Champ d'application;
- section 2 – Conformité;
- section 3 – Références;
- section 4 – Définitions;

- section 5 – Constitutions que doit remplir le système biométrique permettant l'établissement des PIM.

La section 5 se subdivise elle-même en quatre sous-sections, à savoir:

- section 5.1 – Conditions que doit remplir le système biométrique d'établissement des PIM à partir des minuties, empreintes digitales;
- section 5.2 – Prescriptions relatives au code-barres utilisé sur les PIM;
- section 5.3 – Prescriptions relatives à la vérification des données biométriques des PIM;
- section 5.4 – Prescriptions relatives aux bases de données concernant les PIM.

0. Introduction

0.1. Principes de base de l'élaboration des documents

A la suite des attaques terroristes du 11 septembre 2001, l'Organisation internationale du Travail a pris des mesures pour réviser la convention (n° 108) sur les pièces d'identité des gens de mer, 1958, selon une procédure accélérée. Le nouvel instrument, à savoir la convention (n° 185) sur les pièces d'identité des gens de mer (révisée), 2003, qui a été adoptée par la Conférence internationale du Travail en juin 2003, propose des normes de sécurité modernes visant à résoudre la question urgente posée par le refus d'admettre les gens de mer sur le territoire des pays visités par leurs navires en vue de prendre un congé à terre, de passer en transit, de gagner un navire ou de changer de navire. L'une de ces normes de sécurité est un modèle biométrique correspondant à une empreinte digitale traduite sous formes de chiffres dans un code-barres «répondant à une norme à déterminer» (convention n° 185, annexe I).

Dans une résolution adoptée par la Conférence internationale du Travail en juin 2003, il a été demandé au Directeur général que les institutions compétentes «prennent rapidement des mesures en vue de l'élaboration d'une norme interopérable au plan mondial» sur le modèle biométrique mentionné ci-dessus, particulièrement en coopération avec l'Organisation de l'aviation civile internationale. Lors d'une réunion qui s'est tenue à l'OIT en septembre 2003, réunion à laquelle participaient les représentants des gouvernements, des armateurs et des gens de mer, ainsi que ceux de l'OACI et de l'ISO, il est apparu clairement que l'OACI, qui œuvre à l'élaboration d'une recommandation privilégiant une solution biométrique différente (voir ci-dessous) en tant que norme applicable aux passeports lisibles à la machine, n'était pas à même de prendre une part active à l'élaboration du modèle exigé par la nouvelle PIM. Il a été également noté que le temps limité dont on disposait avant l'entrée en vigueur de la convention n° 185 interdisait de recourir à la procédure normale d'élaboration d'un tel modèle dans le cadre de travail de l'ISO et de la CEI.

Aussi le BIT a-t-il commandé le présent rapport technique, intitulé ILO SID-0002 rev. 02, pour exposer les exigences strictes imposées par la convention n° 185 au sujet de l'identification personnelle des gens de mer par voie biométrique. Les auteurs soumettent ce rapport sous la forme d'un profil biométrique définissant la norme applicable à la création et au stockage de gabarits biométriques créés à partir des minuties digitales dans le code-barres bidimensionnel PDF417 des PIM de la prochaine génération et dans les bases de données électroniques nationales des Membres (voir respectivement annexes I et II à la convention n° 185). Ce profil biométrique se présente sous une forme largement

conforme à la norme de l'ISO et peut évoluer vers une norme, puis vers un document d'achat, à la suite d'une discussion internationale et d'une harmonisation des prescriptions.

0.2. Travaux connexes

Tout un ensemble d'études, d'expérimentations, de programmes pilotes et de produits ont été réalisés au cours des dernières années pour accélérer les opérations d'inspection aux points de passage des frontières. Nombre de travaux incorporent les techniques biométriques dans les documents de voyage et les pièces d'identité internationales de la prochaine génération. L'OIT a élaboré la convention n° 185 pour définir les normes des pièces d'identité des marins de la prochaine génération, qui contiendront des données d'identification personnelle du marin (détenteur du document) fondées sur la biométrie et stockeront des gabarits biométriques dans un code-barres imprimé.

Avant le 11 septembre 2001, le secteur de la biométrie avait lancé divers projets d'élaboration de normes pour faciliter la mise au point de produits et de systèmes biométriques interopérables, ainsi que l'échange de données biométriques entre les produits et les systèmes, et les normes à respecter pour garantir l'intégrité et la confidentialité des données biométriques.

- ISO/IEC FCD 19784 – Technologies de l'information – Interface relative au programme d'application biométrique (BioAPI) (ISO/IEC JTC 1 SC37 N numéro 55¹, datée du 17 décembre 2002), qui propose une interface de programmation de l'application garantissant que les produits et systèmes conformes peuvent interopérer entre eux (il s'agit aussi d'une norme de l'Institut américain de normalisation et de l'International Committee for Information Technology Standards: ANSI/INCITS 358:2002 – Technologies de l'information – Spécification BioAPI).
- ISO/IEC CD 19785 – Technologies de l'information – Cadre relatif aux formats d'échange biométriques communs (CBEFF) (ISO/IEC JTC1 SC37 N 208, datée du 14 juillet 2003).
- ISO/IEC CD 19794-2 – Formats d'échange de données biométriques – Partie 3: données relatives aux minuties digitales (ISO/IEC JTC 1 SC37 N 340, datée du 7 octobre 2003).
- Norme de l'Organisation de l'aviation civile internationale (OACI) (document 9303) applicable aux documents de voyage à lecture optique, établie à la demande du comité technique ISO/IEC JTC1 SC17.

Note: La recommandation la plus récente de l'OACI consiste à inclure la technologie des cartes à puce sans contact dans les documents de voyage de la prochaine génération, ainsi qu'une ou plusieurs donnée(s) biométrique(s) (les données biométriques faciales sont prescrites par la norme MRTD de l'OACI, et l'on pourrait également inclure soit une empreinte digitale, soit un système de reconnaissance de l'iris. Bien que la PIM de l'OIT soit un document d'identité (et non un document de voyage), l'Organisation s'efforcera dans la mesure du possible de suivre le projet de norme de l'OACI relatif aux documents de voyage à lecture optique de la prochaine génération. Il est important de noter que les PIM de la prochaine génération utiliseront une technologie fondée sur les codes-barres pour stocker les données

¹ Pour consulter le document ISO/IEC JTC 1 SC37, consultez le site Internet www.jtcl.org, sélectionnez le sous-comité 37, allez dans la partie relative aux documents et tapez le numéro de document dans la zone N Number).

biométriques (et non la technologie faisant appel à des circuits intégrés incorporés, recommandée par la norme MRTD de l'OACI). Cette différence a des conséquences importantes pour le profil biométrique de la PIM. Si le système de stockage utilisant les codes-barres est moins coûteux que le système utilisant les circuits intégrés, le premier (SID PDF417) offre une capacité de stockage nettement moindre que le second.

Comme la PIM de l'OIT de la prochaine génération utilisera la technologie fondée sur les codes-barres pour stocker les données biométriques et répondre aux normes d'interopérabilité de ce document, ce profil biométrique définit le format du stockage des modèles d'empreintes digitales utilisant le code-barres PDF417. Aussi les normes ISO/IEC 15438:2001 (symbologie du code-barres PDF417) et ISO/IEC FDIS 15415 (qualité d'impression correspondant au code-barres PDF417) sont-elles fondamentalement applicables à ce profil biométrique.

Prises ensemble, ces différentes normes (ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC CD 19794-2 et ICAO 9303) représentent les fondations sur lesquelles il est possible d'édifier les moyens biométriques des systèmes relatifs aux PIM. D'autres normes déjà élaborées (comme la norme ANSI/INCITS 358:2002 – Technologies de l'information – Spécification BioAPI) ou en cours d'élaboration, parallèlement à cette norme (comme la norme ISO/IEC WD 19794-4 – Formats d'échange de données biométriques – Partie 4: format d'échange fondé sur l'image des empreintes digitales (ISO/IEC JTC 1 SC37 N 341, datée du 7 octobre 2003) présenteront également une utilité (voir ci-dessous).

0.3. Détermination de l'option biométrique fondée sur les empreintes digitales

La convention n° 185 de l'OIT dispose que la PIM doit être interopérable sur le plan international. Aussi l'OIT devait-elle choisir entre les données biométriques fondées sur l'image, les *minuties* ou le *dessin papillaire* comme base de la pièce d'identité des marins de la prochaine génération. Deux rapports techniques ont été établis, et les comités techniques correspondants ont donné leur avis à l'appui de la décision de l'Organisation. Le présent rapport (SID-0002) expose les prescriptions techniques de l'option biométrique fondée sur les *minuties*, option qui n'a pas été retenue parce qu'elle ne représente pas la solution la mieux adaptée aux besoins de l'OIT. Les arguments avancés pour retenir l'option fondée sur le *dessin papillaire* digital figurant à la section 5.1.3 du rapport ILO SID-0001 rev. 05, intitulée *Saisie des empreintes digitales*.

L'OIT se réserve le droit de reconsidérer cette décision à mesure que les normes internationales et les options technologiques allant à l'appui de la convention n° 185 évoluent.

1. Champ d'application

Le présent rapport technique (ILO SID-0002), intitulé *Profil biométrique créé à partir des minuties digitales aux fins de l'établissement des pièces d'identité des gens de mer*, donne des orientations en vue de l'incorporation des technologies biométriques fondées sur les caractéristiques des empreintes digitales dans les PIM, conformément à la convention (n° 185) sur les pièces d'identité des gens de mer (révisée), 2003. Les auteurs ont fait appel aux ressources complémentaires suivantes: 1) la note d'orientation relative au modèle biométrique établie par la réunion informelle sur la biométrie en vue des PIM, qui s'est tenue les 29 et 30 septembre 2003; 2) des documents d'information supplémentaires; 3) la réunion relative à une consultation technique qui s'est tenue à Genève du 5 au 7 décembre 2003; 4) les avis d'experts du terrain.

La biométrie sera utilisée pour renforcer le lien existant entre la PIM et le marin qui la détient.

Le rapport est structuré comme suit: prescriptions relatives à la conformité du profil biométrique (section 2); Références techniques (section 3); définitions (section 4); et prescriptions biométriques relatives aux PIM (section 5). Cette dernière section se subdivise en quatre sous-sections:

- la sous-section 5.1, intitulée *Prescriptions biométriques établies à partir des minuties digitales*, qui comprend l'enrôlement et la saisie des empreintes digitales, ainsi que le modèle d'empreinte digitale à incorporer dans les pièces d'identité des gens de mer de la prochaine génération;
- la sous-section 5.2, intitulée *Prescriptions relatives au code-barres utilisé sur les PIM*, qui comprend le format des codes-barres, la technique d'impression et les spécifications de cette impression, la technique de lecture et les caractéristiques physiques des codes-barres;
- la sous-section 5.3, intitulée *Prescriptions relatives à la vérification des données biométriques des PIM*, qui expose la procédure de vérification de l'identité biométrique;
- la sous-section 5.4, intitulée *Prescriptions relatives aux bases de données concernant les PIM*, qui expose les prescriptions relatives aux bases de données concernant les codes-barres et celles relatives aux bases de données électroniques nationales concernant les PIM.

L'annexe A expose en détail le format des codes-barres concernant les PIM. L'annexe B décrit le format des données biométriques relatives aux minuties. L'annexe C comprend un exemplaire des normes suivantes: ISO/IEC CD 19794-2 – Formats d'échange de données biométriques – Partie 2: données relatives aux minuties digitales (ISO/IEC JTC 1 SC37 N 340, datée du 7 octobre 2003). L'annexe D comprend un exemplaire des normes suivantes: ISO/IEC WD 19794-4 – Formats d'échange des données biométriques – Partie 4: format d'échange fondé sur l'image des empreintes digitales (ISO/IEC JTC 1 SC37 N 341, datée du 7 octobre 2003).

Comme ce format de stockage des empreintes digitales a été élaboré en conformité avec les documents relatifs aux projets de normes ISO, *le présent document primera pour ce qui est des pièces d'identité des gens de mer*, au cas où l'évolution de l'un ou l'autre de ces projets de normes semblerait indiquer qu'ils sont en contradiction.

Les questions ci-dessous sont exclues du champ d'application du présent rapport technique:

- 1) processus d'ensemble relatif aux systèmes d'identification des gens de mer faisant appel aux techniques biométriques;
- 2) critères de validation de l'identité des gens de mer et de leur titre professionnel;
- 3) critères d'émission des PIM;
- 4) opportunité de faire appel à d'autres techniques biométriques fondées sur les minuties digitales;
- 5) critères concernant «les autres caractéristiques relatives à la sécurité» qui sont mentionnées dans l'introduction à l'annexe I de la convention n° 185;

- 6) questions relatives à l'environnement marin, y compris celles qui concernent la corrosion saline (ces questions devraient toutefois être abordées dans le cadre des spécifications relatives à la fourniture des PIM);
- 7) évaluation des risques liés à l'application.

2. Conformité

Un système biométrique est conforme à la norme s'il satisfait à toutes les prescriptions définies à la section 5, intitulée *Conditions que doit remplir le système biométrique d'établissement des PIM*, à l'annexe A, *SID minutiae-based fingerprint bar code format*, et à l'annexe B, *SID bar code minutiae-based fingerprint storage format*.

Toutes les techniques et caractéristiques biométriques ne conviennent pas aux pièces d'identité des gens de mer, compte tenu des exigences de l'OIT et du degré d'évolution des normes internationales relatives aux techniques biométriques applicables aux empreintes digitales à la date de la présente publication. La norme correspond aux prescriptions permettant d'obtenir l'interopérabilité internationale des composants biométriques fondés sur les minuties digitales des pièces d'identité des gens de mer de la prochaine génération.

3. Références

Le présent profil biométrique est élaboré avant que n'ait été effectuée la mise au point définitive des projets de normes qui s'y rapportent. Tout projet de norme cité dans la présente section indique le numéro de document figurant dans la norme SC37 et la date de publication du projet dont il est question. Un exemplaire de tous les projets de *normes contraignantes* mentionnés (voir la section 3.1) est inclus en annexe au présent document. Comme ce format de stockage des empreintes digitales a été élaboré en conformité avec les documents relatifs aux projets de normes ISO, *le présent document primera pour ce qui est des pièces d'identité des gens de mer* au cas où l'évolution de l'un ou l'autre de ces projets de normes semblerait indiquer qu'ils sont en contradiction.

3.1. Normes contraignantes

- a) ISO/IEC FCD 19784 – Technologies de l'information – Interface relative au programme d'application biométrique (ISO/IEC JTC 1 SC37 N numéro 55, datée du 17 décembre 2002).
- b) ANSI/NIST-ITL 1-2000 – Format des données relatives à l'échange d'informations concernant les empreintes digitales – Tableau 5.
- c) ISO/IEC FDIS 15415 – Technologies de l'information – Techniques d'identification automatique et de saisie des données – Spécifications des tests de qualité de l'impression des codes-barres – Deux symboles dimensionnels.
- d) ISO/IEC 15438:2001 – Technologies de l'information – Techniques d'identification automatique et de saisie des données – Spécifications de la symbologie des codes-barres – PDF417.
- e) ISO/IEC WD 19794-3 – Formats d'échange de données biométriques – Partie 2: Données relatives aux minuties digitales (ISO/IEC JTC 1 SC37 N 340, datée du 7 octobre 2002).

- f) ISO/IEC WD 19794-4 – Formats d'échange de données biométriques – Partie 4: Format d'échange fondé sur une image des empreintes digitales (ISO/IEC JTC 1 SC37 N 341, datée du 7 octobre 2003).
- g) ISO/IEC 8859-15:1999 – Technologies de l'information – Jeux de caractères graphiques codés sur un seul octet – Partie 15: Alphabet latin n° 9.
- h) ISO 3166-1:1997 – Codes de représentation des noms de pays et de leurs subdivisions – Partie 1: Codes de pays.
- i) ISO/IEC 9945-1:2003 – Technologies de l'information – Interface pour la portabilité des systèmes (POSIX) – Partie 1: Définitions de base.

3.2. Documentation

- j) Document de l'OACI 9303 – Documents de voyage à lecture optique (Partie 1, 5^e édition, 2003; Partie 3, 2^e édition, 2002).
- k) ANSI/NIST-ITL-1-2000, Format des données types pour l'échange d'informations relatives aux empreintes digitales, au visage, aux cicatrices et aux tatouages (SMT).
- l) ISO/IEC 7810:2003 – Cartes d'identification – Caractéristiques physiques.

3.3. Normes et documents complémentaires à élaborer ou à privilégier en vue d'une utilisation par les gens de mer

- m) Norme relative aux demandes d'octroi de PIM.
- n) Norme relative aux tests et aux déclarations concernant les performances et l'interopérabilité des PIM.
- o) Document d'orientation complet et facile à consulter sur la prise des empreintes digitales, en vue d'aider le personnel d'enrôlement et de vérification à produire des résultats cohérents et fiables.

4. Définitions

Les auteurs se sont efforcés de faire en sorte que les termes, définitions, symboles et abréviations utilisés dans le présent rapport technique soient conformes à la norme sur l'harmonisation du vocabulaire de la biométrie en cours d'élaboration au sein du groupe de travail 1 d'ISO/IEC JTC 1 SC 37. Certains termes utiles sont définis ci-après pour faciliter la lecture de ce document.

4.1. Termes et définitions

4.1.1. Profil d'application

Sous-ensembles conformes ou ensembles de normes de base utilisés pour exécuter certaines fonctions précises. Les profils d'application définissent l'utilisation de certaines options des normes de base et fournissent une base pour l'échange de données entre applications et l'interopérabilité des systèmes.

4.1.2. Biométrie

Relevant du domaine de la biométrie, utilisé comme adjectif.

Note (pour l'anglais): «biometric» ne doit plus être utilisé comme substantif.

4.1.3. Authentification biométrique/authentifier biométriquement

Authentifier l'identité d'un individu au moyen d'un système de vérification ou d'identification biométrique.

4.1.4. Bloc de données biométriques (BDB)

Bloc de données mémorisées sous un format prédéfini contenant un ou plusieurs échantillons ou gabarits biométriques.

4.1.5. Identification biométrique/identifier biométriquement

Comparer un échantillon biométrique à l'ensemble des échantillons traités et mémorisés dans la base de données biométriques afin de l'apparier à l'un d'entre eux et d'obtenir un indice de comparaison indiquant le degré de similitude des échantillons comparés.

4.1.6. Enregistrement d'informations biométriques

Structure de données contenant un bloc de données biométriques, des informations précisant le format sous lequel elles ont été enregistrées et, éventuellement, d'autres informations comme par exemple si le BDB est numériquement signé ou crypté.

4.1.7. Enregistrement de données biométriques d'échange

Ensemble de données concernant une seule personne, contenant des informations biométriques (voir 4.1.6) ainsi que d'autres informations concernant spécifiquement les systèmes, applications ou fonctions relatifs aux pièces d'identité des marins.

4.1.8. Echantillon biométrique

Données recueillies à l'aide d'un lecteur biométrique, enregistrées soit directement soit après traitement.

4.1.9. Vérification biométrique/vérifier biométriquement

Opération consistant à vérifier qu'un échantillon biométrique est semblable à l'échantillon biométrique précédemment traité et mémorisé correspondant à l'identité que prétend posséder l'intéressé, en appariant les gabarits pour obtenir un indice qui est ensuite comparé à un seuil de validation.

4.1.10. Enrôlement biométrique

Procédé consistant à recueillir un échantillon biométrique, ou plusieurs, auprès d'un individu et à traiter puis à mémoriser un ou plusieurs de ces échantillons ainsi que d'autres données relatives à l'identité de l'individu concerné.

4.1.11. Code des noms de pays

Codes numériques à trois chiffres spécifiés dans la norme ISO 3166-1.

4.1.12. Intégrité des données

Le système la garantit lorsque les données enregistrées sur un support physique, tel qu'une PIM ou une base de données électroniques nationale sur les PIM, ne peuvent être modifiées sans que cela ne soit décelé et sans que l'origine de l'altération ne puisse être détectée.

4.1.13. Confidentialité des données

Le système la garantit lorsque l'accès aux données enregistrées sur un support physique tel qu'une PIM ou une base de données électroniques nationale sur les PIM, ou le traitement de ces données, sont réservés à certaines personnes ou pour des applications expressément autorisées, dotées de la capacité technologique nécessaire.

4.1.14. Interopérabilité à l'échelle mondiale des données biométriques enregistrées sur les PIM

Acceptation à l'échelle mondiale du bloc de données biométriques relatives aux empreintes digitales mémorisé sur le code-barres bidimensionnel imprimé sur la PIM, aux fins d'authentifier l'identité du marin.

4.1.15. Terminaison zéro

Finissant par un octet zéro (0 x 00).

4.1.16. Temps réel

Caractérise un mode opératoire informatique selon lequel l'ordinateur recueille des données, les traite et en utilise les résultats pour le contrôle instantané d'un procédé.

4.1.17. Secondes depuis l'époque

Secondes depuis l'époque, dans un entier non signé de 32 bits, de la journée spécifiée comme défini dans la norme ISO/IEC 9945-1:2003, section 4.14. Toute seconde d'une journée donnée est acceptable mais, si elle n'est pas effectivement connue, l'application PIM se calera par défaut sur la première seconde de cette journée.

4.1.18. Présent

Conformément à la pratique juridique, le terme «présent» indique une obligation.

4.1.19. Conditionnel

Conformément à la pratique juridique, le terme «conditionnel» indique une recommandation.

4.1.20. Jeux de caractères graphiques

Jeux de caractères graphiques d'encodage conformes à la norme ISO 8859-15:1999 (alphabet latin).

5. Conditions que doit remplir le système biométrique permettant l'établissement des PIM

5.1. Conditions que doit remplir le système biométrique d'établissement des PIM à partir des minuties digitales

Les gabarits biométriques des minuties de deux doigts du marin destinataire du document sont imprimés sous forme chiffrée dans un code-barres conforme à la norme énoncée dans le présent document. La convention n° 185 de l'OIT fixe un certain nombre de préconditions auxquelles doit répondre le système finalement sélectionné qui sont présentées ci-après, suivies d'un exposé de ce que leur respect présuppose selon les auteurs du rapport.

- «Les données biométriques peuvent être recueillies sans aucune intrusion dans la vie privée des intéressés, sans désagrément pour eux, sans risque pour leur santé et sans atteinte à leur dignité.» (Convention de l'OIT n° 185, art. 3, paragr. 8 a)).

On suppose que les marins ne percevront pas la saisie et la vérification de leurs empreintes comme une intrusion dans leur vie privée ou une offense à leur dignité. L'ergonomie des appareils de saisie des données biométriques et de lecture des codes-barres sera telle que le marin ne subira aucun désagrément. Les risques pour la santé des marins seront évalués tant au stade de la saisie initiale que des vérifications ultérieures et les appareils seront régulièrement aseptisés pour prévenir tout risque de propagation de microbes par contact avec leurs éléments de sorte que leur utilisation ne présente pas plus de danger pour la santé que le contact avec une poignée de porte par exemple.

- «Les données biométriques sont visibles sur la pièce d'identité et ne peuvent être reproduites à partir du modèle ou d'autres représentations.» (Convention de l'OIT n° 185, art. 3, paragr. 8 b)).

Il doit être suffisamment difficile de reconstituer une empreinte digitale en tant que telle (c'est-à-dire «une image d'empreinte digitale») ou de fabriquer un dispositif frauduleux pouvant être utilisé pour dénaturer l'intention ou falsifier la présence du marin à partir des données biométriques enregistrées dans le code-barres. Les données biométriques des empreintes digitales sont par ailleurs considérées comme étant visibles lorsque le code-barres dans lequel elles sont enregistrées est imprimé sur la génération suivante de PIM.

- «Le matériel nécessaire au recueil et à la vérification des données biométriques est facile à utiliser et est généralement accessible aux gouvernements à faible coût.» (Convention de l'OIT n° 185, art. 3, paragr. 8 c)).

On suppose ici que la bonne ergonomie des équipements biométriques en garantira la facilité d'utilisation pour ceux qui sont chargés de la mise en œuvre des systèmes et les utilisateurs. On suppose par ailleurs que le choix qu'a fait l'OIT d'un mode de stockage dans un code-barres des données biométriques relatives aux minuties satisfait à la demande d'un système «généralement accessible aux gouvernements à faible coût».

- «Le matériel nécessaire à la vérification des données biométriques peut être utilisé de manière commode et fiable dans les ports et dans les autres lieux, y compris les navires, où les autorités compétentes effectuent normalement le contrôle de l'identité.» (Convention de l'OIT n° 185, art. 3, paragr. 8 d)).

On suppose que les systèmes d'enregistrement des données biométriques et les lecteurs de cartes pourront être utilisés de manière fiable à bord des navires, dans les ports et autres lieux sans être indûment sensibles à la salinité corrosive de l'air marin ambiant.

- «Le système, y compris les matériels, les technologies et les procédures, dans lequel les données biométriques sont utilisées permet d'obtenir des résultats uniformes et fiables en matière d'authentification d'identité.» (Convention de l'OIT n° 185, art. 3, paragr. 8 e))

Par résultats «uniformes», on entend que le système biométrique est conforme aux prescriptions du présent rapport technique pour répondre à l'exigence d'interopérabilité et qu'il fonctionnera aussi bien pour l'ensemble des marins. On suppose également que les systèmes biométriques commerciaux permettront une «authentification de l'identité» (au sens de «vérification de l'identité») fiable de l'ensemble des marins utilisant ces systèmes.

5.1.1. Procédure d'enrôlement biométrique

L'ensemble de la procédure de vérification d'identité que permet la PIM de l'OIT ne sera pas traitée dans le présent rapport qui portera essentiellement sur la partie de la procédure relative à l'enrôlement biométrique. Une personne qualifiée chargée de délivrer le document enregistrera dans le système d'enrôlement les informations personnelles dont la liste est donnée à l'annexe A. Une empreinte digitale de l'index de chaque main devrait être saisie². Si l'empreinte de l'index n'existe plus ou est endommagée au point que soit l'on ne peut pas saisir une empreinte fiable, soit on ne peut pas l'enrôler en raison de sa mauvaise qualité, on saisira alors l'empreinte d'un autre doigt ou d'un pouce en veillant à ce que la cohérence et l'efficacité opérationnelles soient maximales sans causer de désagrément au marin. L'ordre de présentation standard des doigts aux fins de l'enrôlement est le suivant:

- index de la main droite,
- index de la main gauche,
- pouce de la main droite,
- pouce de la main gauche,
- majeur de la main droite,
- majeur de la main gauche,
- annulaire de la main droite,
- annulaire de la main gauche,
- auriculaire de la main droite,
- auriculaire de la main gauche.

² La saisie de l'empreinte de deux doigts permet d'améliorer la fiabilité et la solidité du système. L'index est choisi en priorité car, dans la plupart des cas, c'est le doigt que l'on peut placer le plus facilement sur l'appareil de saisie, ce qui garantit au marin le minimum d'inconfort (convention n° 185, art. 3, paragr. 8, première condition préalable).

La personne chargée de délivrer les PIM précisera au moment de l'enrôlement quel est le doigt dont l'empreinte a été saisie et enregistrera cette information dans l'en-tête du gabarit biométrique mémorisé dans le code-barres de la PIM (voir annexe B).

Le système doit soit être doté d'un moyen de mesure automatique de la qualité de la saisie, soit fournir à la personne effectuant l'enrôlement le moyen d'évaluer celle-ci grâce à la signalisation d'un seuil d'acceptabilité permettant de garantir la création de gabarits de bonne qualité. Des empreintes de la meilleure qualité possible devraient être enrôlées et les gabarits d'empreintes digitales devraient être mémorisés de façon à permettre des vérifications fiables. Le marin pourra vérifier que les données biométriques de référence mémorisées sur sa PIM peuvent permettre d'effectuer une vérification biométrique, en particulier sur le lieu de délivrance de son document.

Le système biométrique de saisie d'empreintes digitales doit:

- afficher des messages sur écran lors de la procédure d'enrôlement, adressés à la fois à la personne chargée de délivrer la PIM et au marin, indiquant notamment la marche à suivre, la qualité de la saisie et la manière de positionner le doigt;
- permettre de connaître la teneur et la qualité des gabarits saisis et de les évaluer par rapport à des seuils fixés à l'avance de telle sorte que, si nécessaire, le marin puisse être invité à présenter soit le même doigt pour le réenrôler, soit le doigt suivant;
- donner une indication de la qualité du gabarit d'empreinte digitale saisi et renvoyer à l'opérateur (c'est-à-dire la personne délivrant la PIM) ainsi qu'à la personne enrôlée (c'est-à-dire le marin) une image de l'empreinte digitale enregistrée;
- permettre à la personne chargée de délivrer la PIM de choisir un autre doigt aux fins d'enrôlement si le système ne réussit pas à enregistrer un gabarit d'une qualité acceptable pour un doigt donné;
- permettre au marin de vérifier biométriquement avant l'impression du code-barres sur sa PIM si le gabarit saisi correspond à l'empreinte digitale enrôlée et lui est acceptable au plan opérationnel; une indication positive doit être donnée (identité vérifiée) si la valeur d'appariement est supérieure au seuil fixé aux fins de vérification (voir 5.3.1 ci-après) et une indication négative (identité non vérifiée) si le seuil d'appariement est en deçà du seuil de correspondance;
- fournir une indication du nombre de doigts correctement enrôlés;
- permettre à la personne délivrant la PIM de revoir les données textuelles saisies, de les modifier si nécessaire et d'imprimer le code-barres sur la PIM;
- permettre la vérification biométrique de l'identité du marin à l'aide de la PIM imprimée comme indiqué à la section 5.3.1.

5.1.2. Documentation relative à l'enrôlement biométrique

Une documentation facile à consulter doit être fournie pour que la personne chargée d'effectuer l'enrôlement sache comment procéder pour garantir l'enrôlement d'empreintes digitales de bonne qualité et l'enregistrement de gabarits de bonne qualité.

5.1.3. Saisie des empreintes digitales

L'appareil de saisie des empreintes permettra de recueillir des gabarits biométriques de minuties conformes au tableau 1 de l'annexe A de la norme ISO/IEC WD 19794-4 –

Formats d'échange de données biométriques – Partie 4: Format d'échange de données relatives à des images digitales (ISO/IEC JTC 1 SC37 N 341, du 7 octobre 2003)³ (voir annexe D au présent document pour l'ensemble du projet de norme) avec au minimum un niveau 3⁴ de qualité de saisie des données d'empreinte comme indiqué ci-après:

- résolution du balayage: 197 pixels par cm (500 pixels par pouce);
- nombre de bits par pixel: 8;
- gamme dynamique (niveaux de gris): 220;
- certification: EFTS/F.

Le dispositif de saisie des empreintes doit permettre de produire une image de l'empreinte digitale qui sera focalisée, de préférence, sur la partie centrale de l'empreinte digitale. Cinquante-deux minuties au maximum doivent figurer dans le gabarit de chaque empreinte. «Si le nombre de minuties dépasse le nombre maximal qu'il est possible de traiter sur une carte, une troncature s'impose. Celle-ci se fait en deux étapes. Tout d'abord, on élimine les minuties de mauvaise qualité. Puis, si le nombre de minuties est encore trop important, une troncature peut être opérée en les éliminant de l'enveloppe convexe⁵ de l'ensemble de minuties et avant de les classer dans l'ordre requis pour la carte⁶.»

Lorsque les données relatives à l'image de l'empreinte digitale sont transmises à l'algorithme d'extraction du gabarit, par exemple de l'appareil de saisie vers un ordinateur, elles doivent soit ne pas être comprimées, soit être comprimées de telle sorte qu'il n'y ait aucune perte de qualité.

5.1.4. Gabarit d'empreinte digitale

L'algorithme extraira un gabarit d'empreinte digitale à partir de l'image d'empreinte saisie conformément à la norme ISO/IEC CD 19794-2 – Formats d'échange de données biométriques – Partie 2: Minuties (ISO/IEC JTC 1 SC37 N 340 du 7 octobre 2003). Les gabarits d'empreinte seront enregistrés dans la base électronique nationale de l'Etat Membre (base de données de la convention) et dans le code bidimensionnel PDF417 2-D figurant sur la PIM, lors de la procédure d'enrôlement, et seront utilisés aux fins de comparaison lors de la procédure de vérification.

L'OIT préconisera en priorité l'utilisation de gabarits créés à partir de minuties digitales pour faciliter les recherches dans les bases de données nationales existantes dans le cadre de la procédure de vérification d'identité préalable à la délivrance de la PIM. Parmi les pays Membres qui ont répondu à la demande que leur a adressée le BIT en

³ Il s'agit là d'un projet de norme en cours de révision dans le cadre du groupe de travail 3/ISO/IEC JTC 1 SC37. Nous pensons que les paramètres de qualité du niveau 3 resteront les mêmes lorsque le projet de norme sera finalement approuvé. Toutefois, les paramètres indiqués dans le présent document seront ceux qui primeront pour les PIM.

⁴ Une qualité de niveau 3 pour la saisie des empreintes digitales est acceptable pour des images devant être utilisées pour créer des gabarits d'empreintes réduites aux minuties. Il est à noter que la qualité de la saisie des données relatives aux empreintes digitales est différente de la qualité de l'image imprimée à partir du code-barres figurant sur la PIM.

⁵ L'enveloppe convexe est la forme la plus petite (un polygone) englobant un ensemble de points.

⁶ ISO/IEC CD 19794-2, du 7 octobre 2003 (ISO/IEC JTC 1 SC37 N 340, paragr. 8.3.1).

décembre 2003, beaucoup ont fait savoir qu'ils avaient l'intention d'utiliser les données relatives aux empreintes digitales pour effectuer des recherches dans les bases de données nationales existantes⁷. Ces bases de données sont en règle générale des bases de données IAFIS (International Automated Fingerprint Information Systems) conçues pour faciliter les recherches par des systèmes intégrant des gabarits de minuties.

- D'après l'article 3, paragraphe 8 b), de la convention n° 185: «*les données biométriques [au sens de «données relatives aux empreintes digitales mémorisées dans le code-barres PDF417»] sont visibles sur la pièce d'identité et ne peuvent être reproduites [c'est-à-dire qu'on ne peut reproduire une «image de l'empreinte digitale»] à partir du modèle ou d'autres représentations».*

Les données biométriques concernant le marin seront mémorisées dans le code-barres PDF417 qui sera visiblement imprimé sur la PIM.

Les données biométriques comporteront deux gabarits des minuties de deux doigts enregistrées sur le format indiqué aux annexes B et C du présent rapport.

L'OIT devra vérifier quelles seraient les conséquences d'une imposition d'un gabarit fixe tel que défini aux annexes B et C. Des essais, dont les modalités doivent être définies, devraient permettre de vérifier les conséquences qu'aurait l'imposition d'un gabarit de taille fixe sur les solutions commerciales individuelles ou sur des solutions commerciales multiples. A ce jour, aucun essai officiel n'a été réalisé pour vérifier que le respect des conditions prescrites dans la convention n° 185 de l'OIT n'entraînera pas une baisse de performance des systèmes biométriques.

- D'après l'article 3, paragraphe 8 b), de la convention n° 185: «*les données biométriques [au sens de «données relatives aux empreintes digitales mémorisées dans le code-barres PDF417»] sont visibles sur la pièce d'identité et ne peuvent être reproduites [c'est-à-dire qu'on ne peut reproduire «l'image de l'empreinte digitale»] à partir du modèle ou d'autres représentations».*

La vérification de la performance des systèmes biométriques intégrant des gabarits de minuties portera non seulement sur les conséquences que pourrait avoir l'imposition d'un gabarit de taille fixe, mais également sur le degré de difficulté de la reconstitution de l'image d'une empreinte digitale ou de mise au point d'un dispositif frauduleux pouvant être utilisé pour dénaturer l'intention ou falsifier la présence du marin à l'aide des données enregistrées dans les gabarits de minuties de taille fixe⁸.

Le format du gabarit biométrique de minuties figurant sur la PIM de l'OIT est précisé dans les annexes A, B et C et obéit à la norme ISO/IEC CD 19794-2 – Formats d'échange de données biométriques – Partie 2: Données relatives aux minuties digitales (ISO/IEC

⁷ Le projet de norme actuel de la commission sur le stockage des données relatives aux minuties n'est pas conforme à la norme IAFIS actuelle ni à d'autres normes AFIS; toutefois, il s'inspire des mêmes principes et concepts. Il suffirait d'un simple programme de conversion pour pouvoir utiliser les données afin de procéder à des comparaisons avec les données enregistrées dans les bases des Etats Membres.

⁸ M. Bromba: «On the reconstruction of biometric raw data from template data», 9 juillet 2003. Peut-être téléchargé à partir du site: <http://www.bromba.com/knowhow/temppriv.htm>. C.J Hill: «Risk of masquerade arising from the storage of biometrics», thèse, Université nationale australienne, 2001. Peut-être téléchargé à partir du site: <http://chris.fornax.net/biometrics.html>.

JTC 1 SC37 N 340, 7 octobre 2003). La structure des données mémorisées dans le code-barres de la PIM est en résumé la suivante:

- en-tête conforme à la norme BioAPI – 16 octets;
- en-tête contenant les données relatives au gabarit des minuties – 30 octets;
- gabarits de minuties pour deux doigts – jusqu'à 520 octets⁹;
- représentation numérique des données telles que décrites à l'annexe A – 120 octets;
- nombre total d'octets du code-barres figurant sur la PIM – jusqu'à 686 octets.

5.2. Prescriptions relatives au code-barres utilisé sur les PIM

5.2.1. Format du code-barres

Le code-barres utilisé sur la PIM sera formaté conformément à l'annexe A. Pour les empreintes digitales créées à partir des minuties, il contiendra au maximum 686 octets, auxquels s'ajouteront 64 symboles de données pour un niveau 5 de correction d'erreur. Il comprendra les données du gabarit biométrique ainsi que les informations à imprimer au recto de la PIM, à savoir: l'autorité de délivrance, le numéro d'identification personnel (facultatif), le nom en entier du marin, le numéro unique du document, la date d'expiration du document, la nationalité du marin, la date et le lieu de naissance, le sexe ainsi que le lieu et la date de délivrance du document (voir l'annexe A). Les gabarits biométriques des empreintes de deux doigts du marin seront formatés conformément à l'annexe B, qui définit le bloc de données biométriques de 566 octets au maximum, visé à l'annexe A. Ce bloc de données biométriques de 566 octets au maximum plus l'information d'en-tête de 120 octets définie à l'annexe A composent le code-barres de la PIM, dont le contenu total représente donc 686 octets.

La technologie du code-barres bidimensionnel PDF417 2-D s'appliquera pour les raisons suivantes:

- les symboles PDF417 répondent aux prescriptions relatives à la capacité de stockage de données requise pour cette application;
- les symboles PDF417 peuvent se lire à l'aide d'un scanner bidimensionnel ou d'un lecteur optique standard – CCD ou à laser – et d'un logiciel spécial de décodage. Toutefois, les crayons lecteurs ne pourront pas lire ces symboles. Cette vaste gamme de lecteurs optiques des codes-barres à usage commercial, qui sont d'un prix abordable, facilitera la vérification par la biométrie de l'identité des membres de la communauté des gens de mer.

⁹ Jusqu'à 52 minuties par doigt seront représentées. Si un doigt possède plus de 52 minuties, une troncature sera effectuée conformément à la norme ISO/IEC CD 19794-2 du 7 octobre 2003 (ISO/IEC JTC 1 SC37 N 340, paragr. 8.3.1), où il est dit: «Si le nombre de minuties dépasse le nombre maximal qu'il est possible de traiter sur une carte, une troncature s'impose. La troncature est un procédé en deux étapes. Tout d'abord, on procède à l'élimination des minuties de mauvaise qualité. S'il reste encore un nombre trop élevé de minuties, une troncature sera effectuée en enlevant des minuties de l'enveloppe convexe de l'ensemble de minuties avant de les hiérarchiser dans l'ordre requis pour la carte.»

Les dimensions et l'emplacement du code-barres seront conformes aux spécifications de l'Organisation de l'aviation civile internationale (OACI), telles qu'elles figurent dans son document 9303, Partie 1 (5^e édition, 2003) et Partie 3 (2^e édition, 2002), et telles qu'elles sont mentionnées ci-après pour la commodité du lecteur:

- pour les livrets PIM, la taille maximale du code-barres est de 21,35 mm x 86 mm, zones non imprimées comprises, ainsi que spécifié par l'OACI dans le document 9303, Partie 1 – Passeports lisibles à la machine – IV Spécifications techniques particulières aux passeports lisibles à la machine – Annexe E (normative) – Utilisation de code(s)-barres sur la page de données des passeports lisibles à la machine (MRP);
- pour les cartes PIM, la taille maximale du code-barres est de 27,8 mm x 85,6 mm¹⁰, zones non imprimées comprises (voir le document 9303 de l'OACI, Partie 3 – Les documents de voyage officiels lisibles à la machine de formats 1 et 2 –, Annexe E (normative) à la section IV – Utilisation du/des code(s)-barres optionnels sur le TD-1).

En outre, le code-barres utilisé sur la PIM sera conforme aux spécifications suivantes:

- dimension X: la largeur du module de symboles est comprise entre une valeur minimale de 0,170 mm (plus grande pour remplir, si possible, la zone de carte) et une valeur maximale de 0,175 mm;
- dimension Y: la hauteur de rangée est comprise entre une valeur minimale de 0,511 mm (trois fois la dimension X, voire plus grande pour remplir, si possible, la zone de carte) et une valeur maximale de 0,525 mm;
- un niveau 5 de correction d'erreur, comme recommandé dans les normes ISO/IEC 15438:2001, Annexe E, et dans le document 9303 de l'OACI – Partie 3 (2^e édition, 2002);
- 16 colonnes pour les symboles de données¹¹;
- le nombre de rangées requises (40) pour y faire figurer les données¹².

¹⁰ Cela signifie que la PIM de prochaine génération, qui se présentera sous forme de carte, sera un document de voyage lisible à la machine (MRTD) de format 1 et non pas 2, ainsi que spécifié par le document 9303 de l'OACI – Partie 3 (2^e édition, 2002).

¹¹ Selon les termes de M. Sprague Ackley, expert internationalement reconnu en technologie des codes-barres bidimensionnels PDF417 2-D: « S'il est difficile d'établir avec certitude à partir de quand les systèmes d'imagerie bidimensionnelle commencent à avoir des problèmes avec les symboles PDF 417 dans de nombreuses colonnes, il est quasiment assuré, en revanche, que 25 colonnes de données mettront à mal plusieurs de ces systèmes d'imagerie ». L'utilisation de 16 colonnes de données (20 au total) permettra d'appliquer la technologie de lecture de codes-barres du type scanner bidimensionnel, laissant suffisamment d'espace dans le sens vertical pour intégrer sur la PIM le code-barres et d'autres données.

¹² Ci-après est déterminé par dérivation le nombre de rangées requises dans le format du code-barres utilisé sur la PIM pour les empreintes digitales réduites aux minuties. Les données de la PIM représentent 686 octets. Chaque mot de code peut stocker 1,2 octet. Le nombre de mots de code est donc: $686/1,2 = 572$; 64 mots de code supplémentaires sont nécessaires pour les codes de correction d'erreur de niveau 5, plus un mot de code pour la taille totale du code-barres, ce qui fait au total:

5.2.2. La technologie des imprimantes et les spécifications relatives à l'impression

Le code-barres PDF417 sera imprimé sur la PIM conformément à la norme ISO/IEC 15438:2001. Il est possible d'imprimer les symboles PDF417 du code-barres bidimensionnel avec la plupart des imprimantes de marque de la gamme professionnelle, à transfert thermique, à laser et à jet d'encre. La qualité d'impression du code-barres sur la PIM de prochaine génération sera conforme au projet de norme ISO/IEC FDIS 15415 – Spécification relative au contrôle de la qualité d'impression du code-barres – Deux symboles bidimensionnels, avec la désignation 3.0/05/660. Cette désignation se réfère au niveau 3 de définition des symboles, obtenu avec une ouverture de 0,125 mm pour une longueur d'onde de 660 nanomètres.

Le code-barres de la PIM sera imprimé de telle manière que le document ainsi obtenu soit suffisamment résistant dans l'optique de son utilisation comme document d'identification de gens de mer.

La zone imprimable réservée au code-barres sera conforme aux spécifications de l'OACI telles qu'elles figurent dans le document 9303, Partie 1 (5^e édition, 2003) et Partie 3 (2^e édition, 2002).

5.2.3. La technologie des lecteurs

Les symboles PDF417 utilisés sur les PIM de prochaine génération seront lus à l'aide d'un scanner bidimensionnel ou d'un lecteur standard – CCD ou à laser – et d'un logiciel de décodage spécial capable de lire les codes-barres imprimés conformément aux paragraphes 5.2.1 et 5.2.2 ci-dessus. Cependant, les crayons lecteurs ne pourront pas lire les symboles PDF417.

5.2.4. Caractéristiques physiques des codes-barres

Le «modèle biométrique correspondant à une empreinte digitale traduite sous forme de chiffres dans un code-barres» (convention internationale du travail n° 185, annexe I, paragr. 3 *k*) sera protégé «par un laminat ou une couche de laque, ou par l'application d'une technologie d'image ou d'un support matériel qui garantit une résistance équivalente à la substitution du portrait et d'autres données biographiques». (Convention internationale du travail n° 185, annexe I.) Cette protection améliorera également la durabilité du code-barres.

«Les données biométriques sont visibles sur la pièce d'identité.» (Convention internationale du travail n° 185, art. 3, paragr. 8 *b*.) Cette disposition signifie que les données biométriques sont réputées visibles lorsque le code-barres où sont stockées les données biométriques des empreintes digitales est imprimé sur la PIM de nouvelle génération. Le code-barres est visible s'il est imprimé sur la PIM. Par ailleurs, le marin devra avoir la possibilité de voir une représentation binaire du gabarit traduit en code-barres et de vérifier lui-même les données biométriques en utilisant la PIM comme source de données de référence là où se trouve une autorité délivrant des PIM.

$572 + 64 + 1 = 637$ symboles de données sur le code-barres de la PIM. Il y a 16 colonnes de données. Par conséquent, $637/16 = 40$ rangées requises pour stocker les données du code-barres sur la PIM.

5.3. Prescriptions relatives à la vérification des données biométriques des PIM

5.3.1. Procédure de vérification des données biométriques

Un lecteur balaiera le code-barres de la PIM et lira les informations d'en-tête et les données du gabarit. L'en-tête spécifiera les doigts dont les empreintes sont stockées dans le code-barres.

Le système demandera au marin de placer un premier doigt aux fins de lecture optique du gabarit digital traduit en code-barres.

Si le doigt correspondant au premier doigt enrôlé est manquant, endommagé, n'est pas saisi ou n'obtient pas, après trois essais, un score de correspondance supérieur à la valeur seuil, le système demandera au marin de placer le second doigt enrôlé sur le dispositif de capture biométrique. Si un doigt soumis au balayage direct (live scan) correspond aux gabarits stockés dans le code-barres, le marin aura passé le contrôle avec succès. Si aucun des doigts soumis au balayage direct ne correspond aux gabarits stockés dans le code-barres, le système affichera un message d'échec de vérification. Si, après le troisième essai pour chacun des deux doigts enrôlés, le système affiche un message d'échec, aucune vérification supplémentaire ne sera effectuée avec la même PIM sans l'intervention du personnel autorisé.

Le système de reconnaissance biométrique des empreintes digitales devra:

- retrouver le gabarit à partir du code-barres bidimensionnel PDF417 figurant sur la PIM;
- afficher à l'écran des messages à l'intention de l'autorité de vérification des PIM et du marin pour mener à bien la session de vérification, des messages indiquant la procédure à suivre, des réactions concernant le placement des doigts ainsi que les résultats obtenus;
- demander au marin de placer le doigt approprié sur le capteur d'image;
- comparer l'image saisie des empreintes digitales avec le gabarit correspondant stocké dans le code-barres;
- donner un signal de concordance (identité confirmée) lorsque le score de correspondance est supérieur à la valeur seuil, et un signal de non-concordance (identité non confirmée) lorsque le score de correspondance est inférieur à cette valeur;
- exiger l'intervention du personnel de vérification lorsque, après trois essais par doigt, le marin ne satisfait au contrôle pour aucun des doigts enrôlés.

Le système de reconnaissance biométrique des empreintes digitales devrait:

- avoir un seuil de correspondance tel qu'aussi bien le taux de fausses acceptations que le taux de faux rejets pour le grand public soient inférieurs à 1 pour cent;
- avoir des mesures de contenu et de qualité proportionnelles aux mesures de qualité utilisées pour l'enrôlement;
- prévoir, à titre facultatif, une mesure indiquant la qualité d'enrôlement.

5.3.2. Documentation relative à la vérification des données biométriques

Une documentation conviviale sera fournie au personnel pour qu'il puisse s'initier aux modalités de la procédure de vérification.

5.4. Prescriptions relatives aux bases de données concernant les PIM

5.4.1. Base de données sur les codes-barres

«Les gens de mer disposeront d'un accès facile à des équipements leur permettant d'examiner toute donnée les concernant qui ne peut faire l'objet d'un examen visuel. Cet accès sera donné par l'autorité qui délivre la pièce d'identité ou en son nom.» (Convention internationale du travail n° 185, art. 3, paragr. 9.) Le «modèle biométrique» correspondra «à une empreinte digitale traduite sous forme de chiffres dans un code-barres répondant à une norme» [la présente norme] (convention internationale du travail n° 185, annexe I).

L'autorité qui délivre les PIM permettra aux gens de mer d'accéder aux machines afin de leur permettre d'inspecter les données stockées dans le code-barres bidimensionnel PDF417 utilisé sur la PIM. Le marin aura la possibilité de vérifier si les gabarits d'empreintes digitales stockés dans sa carte correspondent à ceux des doigts enrôlés. Les données autres que les empreintes digitales seront affichées en texte.

5.4.2. Base de données électronique nationale sur les PIM

La convention n° 185 de l'OIT comporte un ensemble de prescriptions auxquelles il convient de se conformer ainsi qu'un ensemble de prescriptions auxquelles chaque Membre devrait se conformer en ce qui concerne la base de données électronique nationale concernant les PIM, qui aura un impact sur la mise en œuvre et l'utilisation du système de reconnaissance biométrique. Ces prescriptions sont mises en exergue ci-après, avec la stratégie de conformité que les auteurs du profil biométrique en question sont censés appliquer.

- «Les renseignements à fournir pour chaque enregistrement dans la base de données électronique que tout Membre doit tenir à jour, conformément aux paragraphes 1, 2, 6 et 7 de l'article 4 de la présente convention [n° 185] [de la Conférence internationale du Travail] doivent se limiter aux éléments suivants:
 1. autorité de délivrance indiquée sur la pièce d'identité;
 2. nom en entier du marin tel qu'inscrit sur la pièce d'identité;
 3. numéro unique du document;
 4. date d'expiration, de suspension ou de retrait de la pièce d'identité;
 5. modèle biométrique figurant sur la pièce d'identité;
 6. photographie (si elle est stockée sous forme numérique);
 7. précisions sur toutes les demandes de renseignements effectuées sur les pièces d'identité des gens de mer. (Convention internationale du travail n° 185, annexe II.)

La base de données électronique nationale contiendra les enregistrements des sept éléments énumérés ci-dessus pour chaque marin à qui une PIM a été délivrée.

- «Aux fins de la présente convention, des restrictions appropriées sont établies afin d'assurer que des données, en particulier photographiques, ne puissent être échangées à moins qu'un mécanisme soit mis en place pour assurer que les normes applicables de protection des données et de la vie privée soient respectées.» (Convention internationale du travail n° 185, art. 4, paragr. 6.)

Des mécanismes de contrôle de l'accès à la base de données seront mis en place afin de protéger les informations concernant les marins de tout accès par des personnes non autorisées ou à des fins détournées.

- «Les renseignements correspondant à chaque point de l'annexe II [de la convention internationale du travail n° 185] sont [seront] saisis dans la base des données au moment où est délivrée la PIM.» (Convention internationale du travail n° 185, annexe III, Partie A, paragr. 3 b) i.)

Les bases de données électroniques nationales des Membres seront actualisées en temps utile chaque fois qu'une PIM est délivrée.

- «Chaque Membre fera en sorte qu'un enregistrement de chaque pièce d'identité des gens de mer, délivrée, suspendue ou retirée par lui, soit conservé dans une base de données électronique. Les mesures nécessaires sont prises pour protéger cette base de données contre toute intervention ou tout accès non autorisé.» (Convention internationale du travail n° 185, art. 4, paragr. 1.) «La pièce d'identité des gens de mer est rapidement retirée par l'Etat qui l'a délivrée s'il est avéré que le marin ne répond plus aux conditions de délivrance fixées par la présente convention.» (Convention internationale du travail n° 185, art. 7, paragr. 2.) «L'autorité qui délivre les PIM devrait établir des procédures appropriées pour protéger la base de données, notamment: permission aux seuls fonctionnaires spécialement autorisés d'avoir accès à une entrée saisie dans la base de données ou d'y apporter un changement une fois que cette entrée a été confirmée par le fonctionnaire qui l'a saisie.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 4.2.2.)

Les bases de données électroniques nationales des Membres assureront une fonction de contrôle de gestion consistant à consigner les transactions, notamment la délivrance, la suspension ou le retrait/annulation de PIM. Des mécanismes de contrôle de l'accès à la base de données seront mis en place afin de protéger les informations concernant le marin de tout accès par des personnes non autorisées ou à des fins détournées. Les fonctionnaires spécialement autorisés de chaque organisation du Membre pourront, dans certaines limites, apporter des changements au journal de vérification; le Membre tiendra à jour les documents attestant ces changements.

- «Lorsqu'une PIM est suspendue ou retirée, des mesures doivent [devront] être prises rapidement pour actualiser la base de données.» (Convention internationale du travail n° 185, annexe III, Partie A, paragr. 3 c)).

Les bases de données électroniques nationales des Etats Membres seront actualisées en temps utile chaque fois qu'une PIM est suspendue ou retirée.

- «Un système de prolongation ou de renouvellement est [sera] mis en place pour répondre aux situations où le marin a besoin d'une prolongation ou d'un renouvellement de sa PIM ou aux situations de perte de PIM.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.) Le requérant ne

devrait pas recevoir de PIM s'il en possède déjà une.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.)

Les Membres mettront en place un système de prolongation et/ou de renouvellement pour répondre aux situations où le marin a besoin d'une prolongation ou d'un renouvellement de sa PIM ou aux solutions de perte de PIM. La prolongation et/ou le renouvellement de la PIM donnera lieu, en temps utile, à une transaction dans la base de données électronique nationale. Si une PIM est rejetée pour cause d'expiration, la base de données électronique nationale fera l'objet d'une vérification tendant à établir si la PIM a été prolongée ou renouvelée. Les gens de mer ne devraient posséder qu'une seule PIM à la fois. La délivrance d'une nouvelle PIM devrait invalider toute PIM que le marin aura reçu antérieurement. Le système de reconnaissance biométrique confirmera si la PIM a été à nouveau enregistrée/délivrée.

- «Un système de renouvellement prématuré devrait s'appliquer lorsqu'un marin sait à l'avance que, compte tenu de la période de son service, il ne sera pas en mesure de présenter sa demande de renouvellement à la date d'expiration.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.1.) «Le requérant ne devrait pas recevoir de PIM s'il en possède déjà une.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.)

Les Membres mettront en place un système de prolongation et/ou de renouvellement pour répondre aux situations où le marin a besoin d'une prolongation ou d'un renouvellement de sa PIM ou aux situations de perte de PIM. Le marin pourra demander une prolongation et/ou un renouvellement à sa convenance dans la mesure où il sait qu'il ne sera pas en mesure de présenter sa demande de renouvellement à la date d'expiration. La prolongation et/ou le renouvellement de la PIM donnera lieu, en temps utile, à une transaction dans la base de données électronique nationale. Si la PIM est rejetée pour cause d'expiration, la base de données électronique nationale fera l'objet d'une vérification tendant à établir si la PIM a été prolongée ou renouvelée. Les gens de mer ne peuvent posséder qu'une seule PIM à la fois. La délivrance d'une nouvelle PIM devrait invalider toute PIM délivrée antérieurement au marin. Le système de reconnaissance biométrique confirmera si la PIM a été à nouveau enregistrée/délivrée.

- «Un système de remplacement devrait s'appliquer dans les cas de perte de PIM. Un document temporaire approprié peut être délivré.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.3.) «Le requérant ne devrait pas recevoir de PIM s'il en possède déjà une.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 3.9.)

Les Membres mettront en place un système de remplacement pour répondre aux situations où un marin perd sa PIM. Le remplacement de la PIM donnera lieu à une transaction en temps réel dans la base de données électronique nationale. Les gens de mer ne devraient posséder qu'une seule PIM à la fois. La délivrance d'une nouvelle PIM devrait invalider toute PIM que le marin aura reçue antérieurement. Le système de reconnaissance biométrique confirmera si la PIM a été à nouveau enregistrée/délivrée. Le marin pourra demander le remplacement de la PIM par un document temporaire, à sa convenance. Ce document temporaire devra être restitué. La base de données électronique nationale sera actualisée en temps utile de manière à tenir compte des changements apportés. Seule sera autorisée à délivrer des documents temporaires l'autorité qui a délivré la PIM d'origine.

- «L'autorité qui délivre les PIM devrait établir des procédures appropriées pour protéger la base de données, notamment l'obligation de faire régulièrement des copies

de la base, qui seront conservées sur des supports tenus en lieu sûr, hors des locaux de l'autorité qui délivre les PIM.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 4.2.2.)

L'autorité de délivrance de chaque Membre fera régulièrement des copies de la base de données électronique nationale, qui seront conservées sur des supports tenus en lieu sûr, hors des locaux de l'autorité qui délivre les PIM.

- «Les informations enregistrées concernant les problèmes de fiabilité ou de sécurité de la base de données électronique, y compris les demandes de renseignements adressées à la base», devraient être tenues à jour par l'autorité de délivrance de chaque Membre.» (Convention internationale du travail n° 185, annexe III, Partie B, paragr. 5.6.5.)

Les bases de données électroniques nationales des Membres assureront une fonction de contrôle de gestion consistant à consigner les problèmes ayant des incidences sur la fiabilité ou la sécurité de la base de données (y compris les demandes de renseignements adressées à la base).

Annexe 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.

Annexe 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, ridge 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 0x000002380104010100203nn0200000008 – 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)).

Annexe 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

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) <p style="text-align: center;">2004-01-07</p> 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: Données 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

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

ISO copyright office
Case postale 56 CH-1211 Geneva 20
Tel: +41 22 749 01 11
Fax +41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

1	Scope	6
2	Conformance.....	6
3	Normative references	6
4	Terms and definitions	6
5	Symbols (and abbreviated terms).....	10
6	Minutiae Extraction	10
6.1	Principle.....	10
6.2	Minutia Type	10
6.3	Minutia Location.....	11
6.3.1	Coordinate System	11
6.3.2	Minutia Placement on a Ridge Ending (encoded as Valley Skeleton Bifurcation Point).....	12
6.3.3	Minutiae Placement on a Ridge Bifurcation (encoded as a Ridge Skeleton Bifurcation Point).....	12
6.3.4	Minutiae Placement on a Ridge Skeleton Endpoint	13
6.3.5	Minutiae Placement on Other Minutiae Types	14
6.4	Minutia Direction.....	14
6.4.1	Angle Conventions	14
6.4.2	Minutia Direction of a Ridge Ending (encoded as Valley Skeleton Bifurcation Point)	14
6.4.3	Minutia Direction of a Ridge Bifurcation (encoded as Ridge Skeleton Bifurcation Point)	14
6.4.4	Minutia Direction of a Ridge Skeleton End Point	14
7	Finger Minutiae Record Format	15
7.1	Introduction	15
7.2	Record Organization	15
7.3	Record Header	15
7.3.1	Format Identifier.....	15
7.3.2	Version Number	15
7.3.3	Length of Record	16
7.3.4	Capture Equipment Certifications	16
7.4	Single Finger Record Format.....	17
7.4.1	Finger Header.....	17
7.4.2	Finger Minutiae Data.....	18
7.5	Extended Data	19
7.5.1	Common Extended Data Fields	19
7.5.2	Ridge Count Data Format.....	20
7.5.3	Core and Delta Data Format.....	22
7.5.4	Zonal Quality Data	24
7.6	Minutiae Record Format Summary	25
8	Finger Minutiae Card Format	27
8.1	Normal Size Finger Minutiae Format	27
8.2	Compact Size Finger Minutiae Format	27
8.3	Number of Minutiae, Minutiae Ordering Sequence and Truncation	28
8.3.1	General Aspects.....	28
8.3.2	Biometric matching algorithm parameters	28
8.3.3	Number of Minutiae.....	28
8.3.4	Minutiae Order.....	29
9	CBEFF Format Owner and Format Types	31

Annex A (normative) Record Format Diagrams	32
A.1 Overall Record Format	32
A.2 Record Header	32
A.3 Single Finger View Minutiae Record.....	33
A.4 Finger Minutiae Data.....	33
A.5 Extended Data	33
Annex B (informative) Example Data Record	34
B.1 Data	34
B.2 Example Data Format Diagrams	35
B.3 Raw Data for the Resulting Minutiae Record	36
Annex C (informative) Handling of Finger Minutiae Card Formats.....	37
C.1 Enrollment	37
C.1.1 Number of minutiae	37
C.1.2 Number of required finger presentations.....	37
C.2 Matching	38
C.2.1 Matching conditions	38
C.2.2 Threshold Value	38
C.2.3 Retry Counter	40
C.3 Security Aspects of Finger Minutiae Presentation to the Card	40

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.

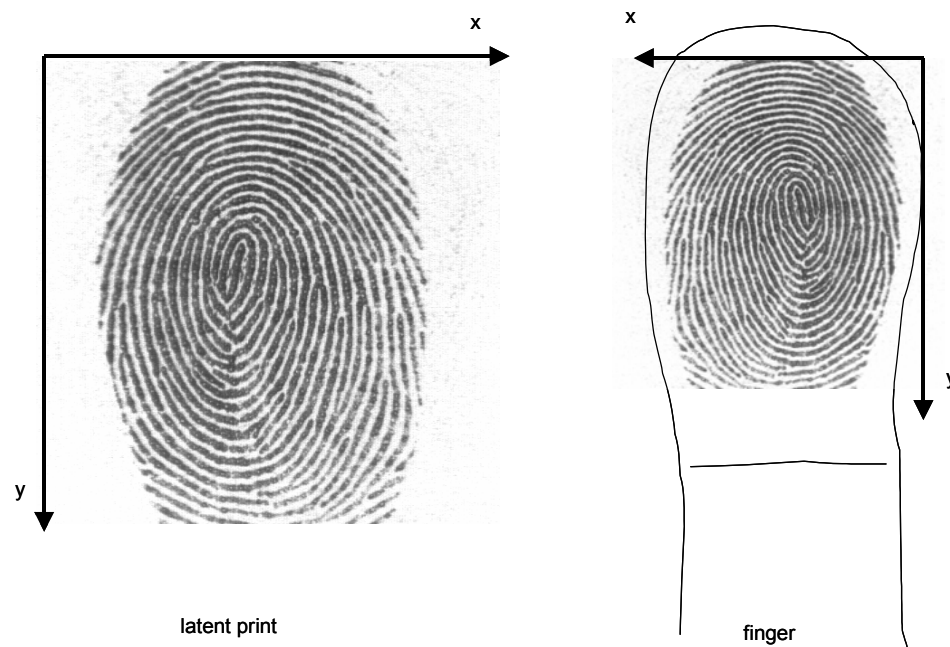


Figure 1 – Coordinate system

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).

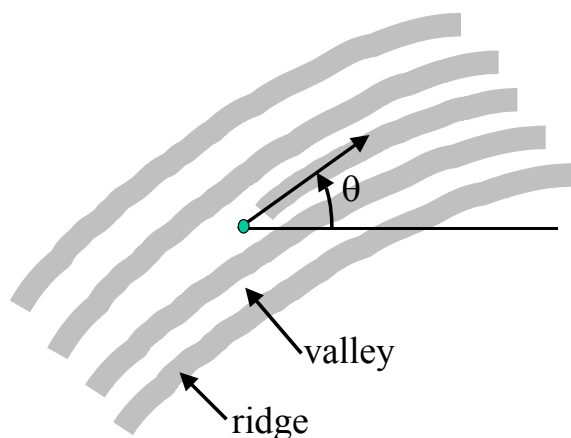


Figure 2 - Location and direction of a ridge ending (encoded as valley skeleton bifurcation point)

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).

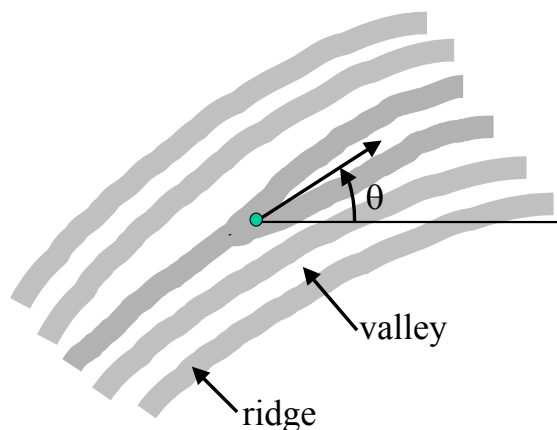


Figure 3 - Location and direction of a ridge bifurcation (encoded as ridge skeleton bifurcation point)

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).

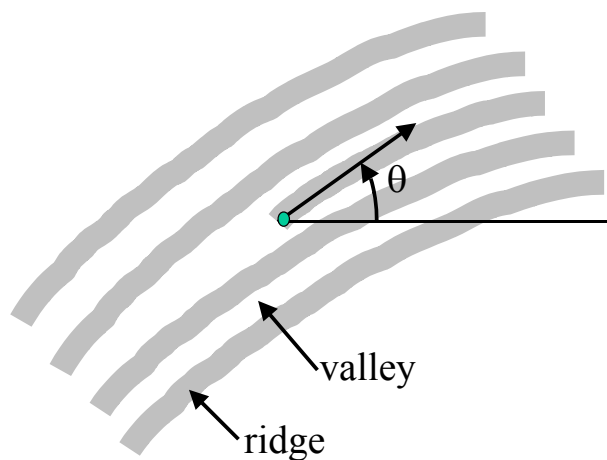


Figure 4 - Location and direction of a ridge skeleton endpoint

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 bifurcation 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
<i>Plain right thumb</i>	11
<i>Plain left thumb</i>	12
<i>Plain right four fingers</i>	13
<i>Plain left four fingers</i>	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

<i>Latent impression</i>	4
<i>Latent tracing</i>	5
<i>Latent photo</i>	6
<i>Latent lift</i>	7
<i>Swipe</i>	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.

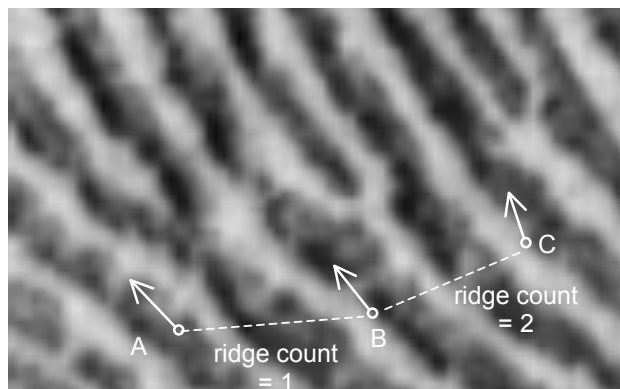


Figure 5 - Example Ridge Count data

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.

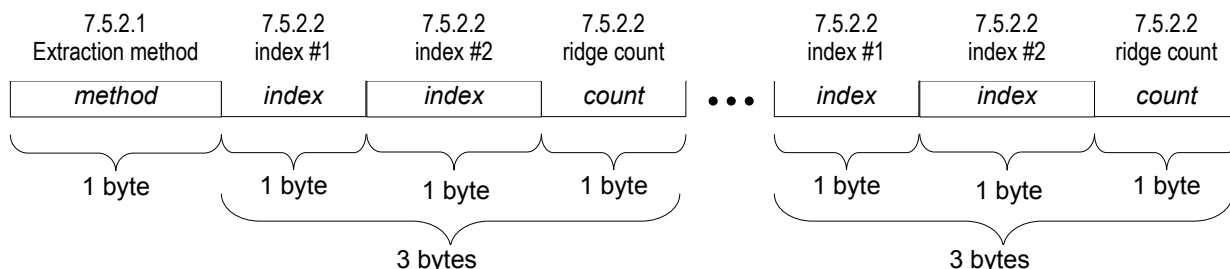
The ridge count data shall be listed in increasing order of the index numbers, as shown in Table 5. There is no requirement that the ridge counts be listed with the lowest index number first. Since the minutiae points are not listed in any specified geometric order, no assumption shall be made about 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

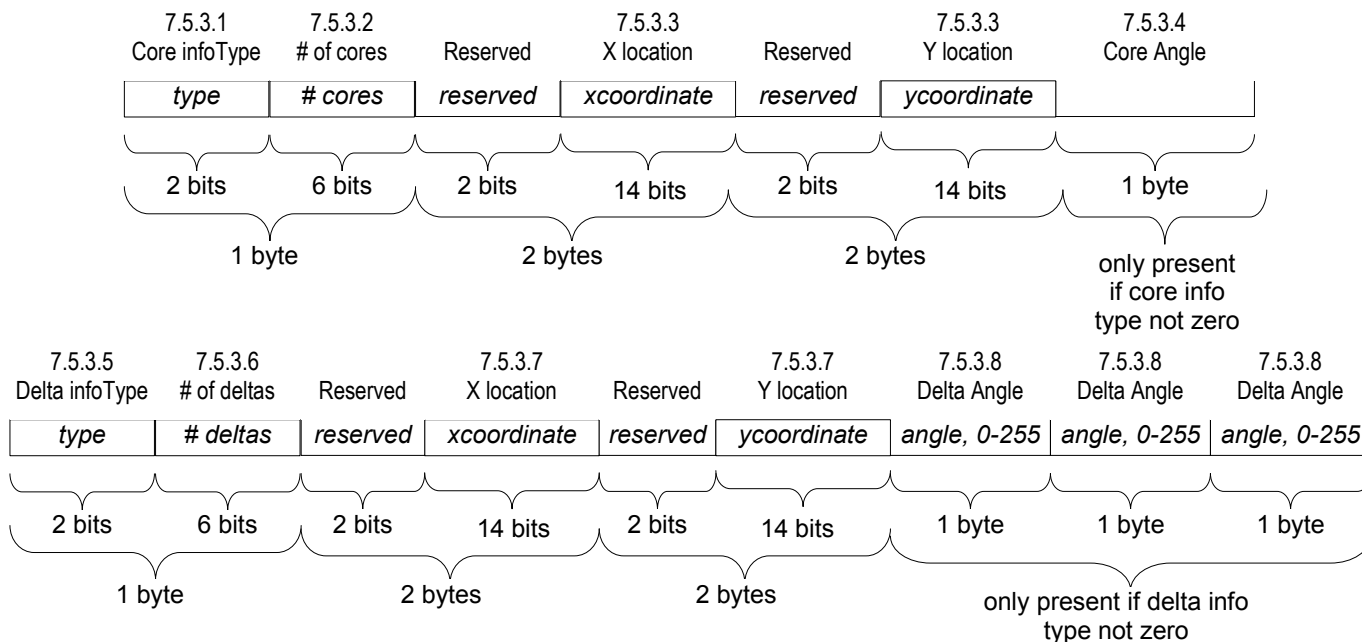
The X coordinate of the delta shall be recorded in the lower fourteen bits of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header.

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.

$$CellDataLength(7.5.4.2) = \text{ceil} \left(\frac{\text{ceil} \left(\frac{XSizeofScannedImage\{7.3.7\}}{CellWidth\{7.5.4.1a\}} \right) \text{ceil} \left(\frac{YSizeofScannedImage\{7.3.8\}}{CellHeight\{7.5.4.1b\}} \right)}{8} \right)$$

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.

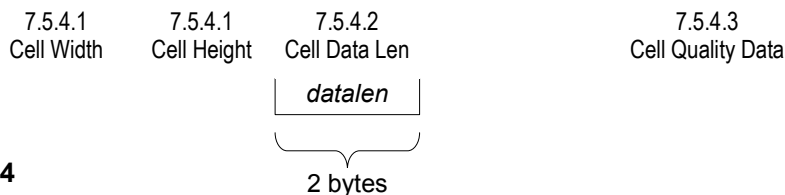
7.5.4.3 Cell Quality Data

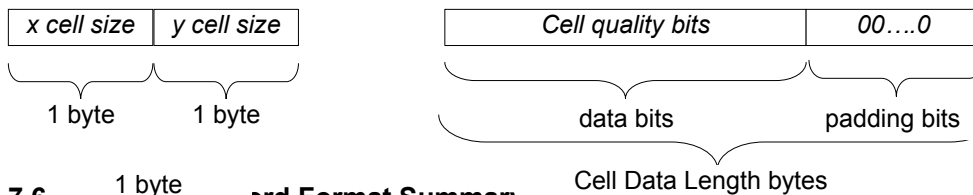
The quality of the fingerprint image in each cell shall be represented by one bit. If the finger image within this cell is of good clarity and significant ridge data is present, the cell quality shall be represented by the bit value '1'. If the cell does not contain significant ridge data, or the ridge 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:





7.6 1 byterd 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
	Type Code for Extended Area	2 bytes		only present if Extended Data Block Length \neq 0
	Length of extended data area	2 bytes		only present if Extended Data Block Length \neq 0
	Extended data area	In prev. field		only present if Extended Data Block Length \neq 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	
		<i>additional ridge counts...</i>		
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 \neq 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 \neq 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 x-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

$$x_{com} = (m_1x_1 + m_2x_2 + \dots) / (m_1 + m_2 + \dots)$$

$$y_{com} = (m_1y_1 + m_2y_2 + \dots) / (m_1 + m_2 + \dots)$$

In the case of a minutiae list, all minutiae are considered equally weighted, which reduces the computation to (assume n minutiae).

$$x_{cm} = (x_1 + x_2 + \dots + x_n) / n$$

$$y_{cm} = (y_1 + y_2 + \dots + y_n) / n$$

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.

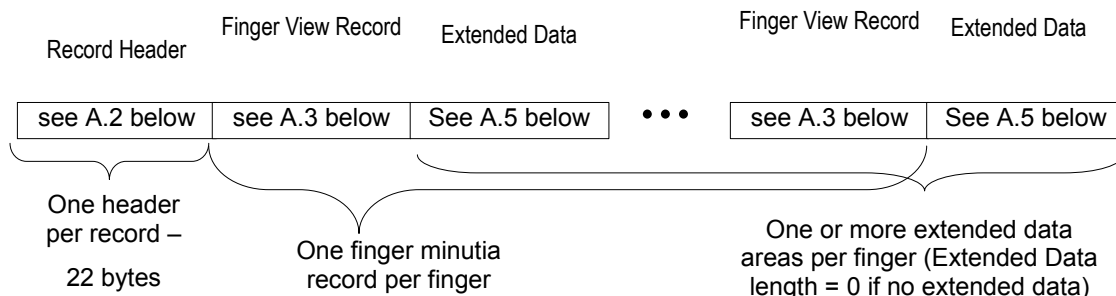
Table 18 — Format types

Format Type	Meaning
'0201'	Finger minutiae record format – no extended data, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton bifurcation points)
'0202'	Finger minutiae record format – extended data, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton bifurcation points)
'0203'	Finger minutiae card format - normal size, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton bifurcation points)
'0204'	Finger minutiae card format - normal size, with - ridge skeleton end points - ridge bifurcations (ridge skeleton bifurcation points)
'0205'	Finger minutiae card format - compact size, with - ridge endings (valley skeleton bifurcation points) - ridge bifurcations (ridge skeleton bifurcation points)
'0206'	Finger minutiae card format - compact size, with - ridge skeleton end points - ridge bifurcations (ridge skeleton bifurcation points)

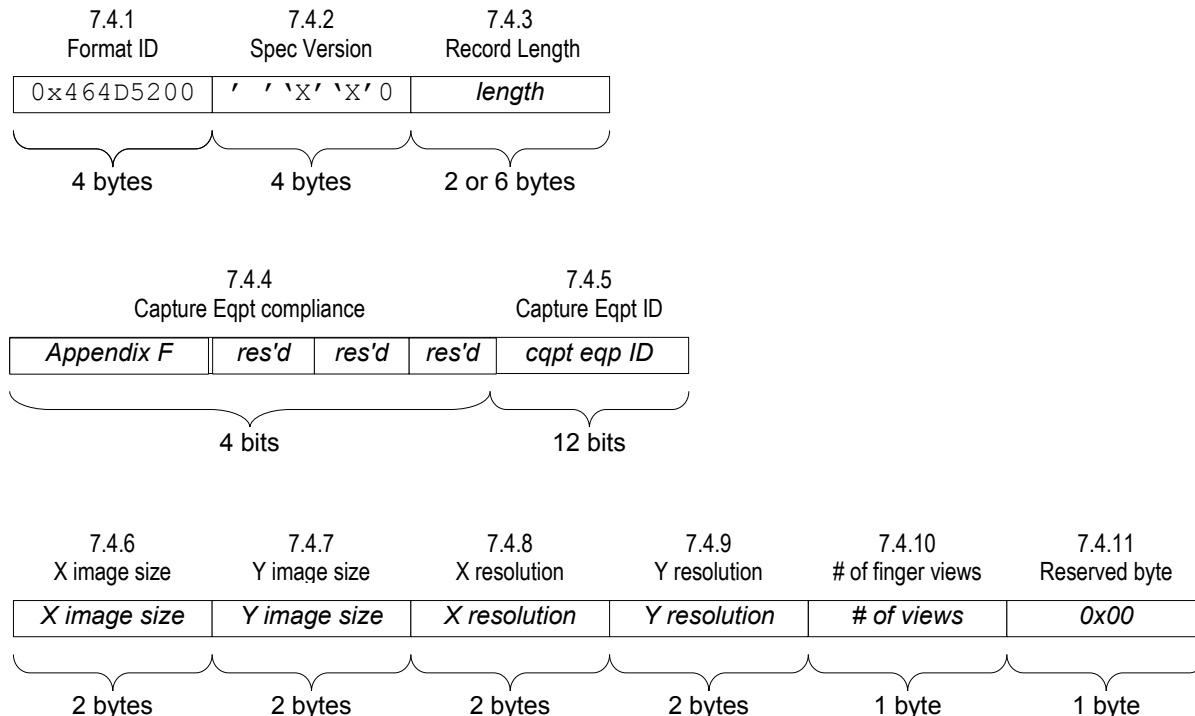
Annex A (normative)

Record Format Diagrams

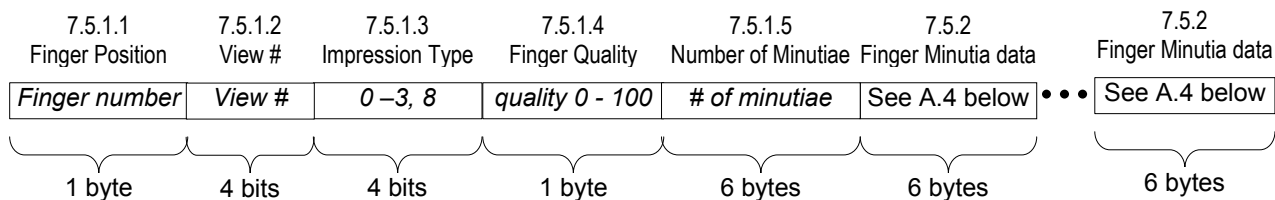
A.1 Overall Record Format



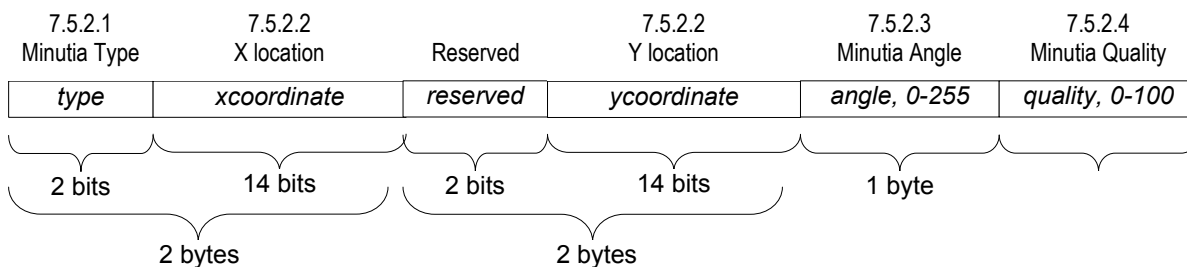
A.2 Record Header



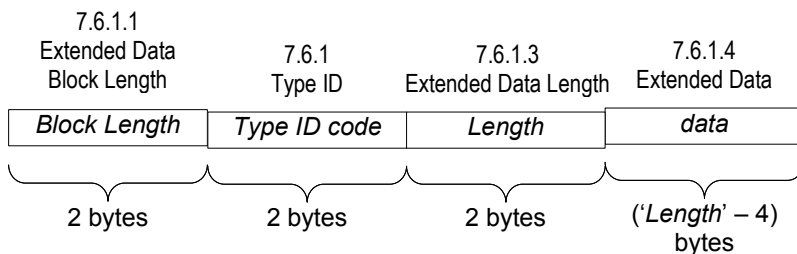
A.3 Single Finger View Minutiae Record



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

Format ID	Spec Version	Record Length	Scanner ID
0x464D5200	'0' '2' '0' '0	0x0000152	0x00B5

X image size	Y image size	X resolution	Y resolution	# of fingers	View number
0x0200	0x0200	0x00C5	0x00C5	0x02	0x00

512 decimal 512 decimal 197 decimal 197 decimal # of fingers reserved

Finger Position	Impression Type	Finger Quality	Number of Minutiae
0x07	0x00	0x5A	0x1B

left index plain live-scan 90 decimal 27 minutiae

Type & X Loc	Y Location	Minutia Angle	Minutia Quality	Extended Area Type ID
0x4064	0x000E	0x70	0x5A	0x0000

0x4000 (type) & 100 decimal 14 decimal 112 decimal 90 decimal

Finger Position	Impression Type	Finger Quality	Number of Minutiae
0x02	0x00	0x46	0x16

right index plain live-scan 70 decimal 22 minutiae

Type & X Loc	Y Location	Minutia Angle	Minutia Quality
0x4028	0x005D	0x00	0x5A

0x4000 (type) & 93 decimal 93 decimal 0 decimal 90 decimal

Extended Area Type ID	Extended Data Length	Extended data
0x0001	0x000A	0x0144BC362143

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:

- A_r : amount of minutiae in the reference data
- A_v : amount of minutiae in the verification data
- A_{vmin} : minimum amount of minutiae required in the verification data
- A_{vmax} : maximum amount of minutiae in the verification data relevant for threshold computation
- T_{min} : minimum threshold value, which denotes the minimum amount of minutiae to be matched for positive verification
- T_{max} : maximum threshold value, which denotes the maximum required amount of minutiae to be matched for positive verification.

T is computed as follows:

$$T = T_{min} + (A_c - A_{vmin}) * (T_{max} - T_{min}) / (A_{vmax} - A_{vmin})$$

with

$$A_c = qA_r + (1 - q)A_v,$$

whereby A_c is the calculated amount of minutiae and the qualifier q the weight for A_r and A_v

and

A_{vmin} = min. amount of minutiae to be presented in a verification process

A_{vmax} = max. amount of minutiae considered relevant in a verification process.

The values of T_{max} , T_{min} , A_{vmax} , A_{vmin} and q chosen for this example are shown in .

Table C.2 - Values for threshold computation (example)

Qualifier q	T_{min}	T_{max}	A_{vmin}	A_{vmax}
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 ($S < T$, T_{min} required = 6)
- a score of 5 matching minutiae leads to positive verification ($S \geq T$), 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 (T_{max} 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*

Annexe D

***ISO/IEC WD 19794-4 (ISO/IEC JTC 1 SC37 N 341,
dated 7 October 2003)***

Voir annexe D de l'annexe I.