INTERNATIONAL LABOUR OFFICE

GB.289/7
289th Session

Governing Body

Geneva, March 2004

SEVENTH ITEM ON THE AGENDA

Follow-up to the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)

1. At its 288th Session in November 2003, the Governing Body discussed a paper prepared by the Office on the follow-up to the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), and to the related resolutions adopted by the International Labour Conference in June 2003. In that paper,[1] the Office referred to urgent action that was needed on two aspects which might influence the decision of governments relating to the early ratification of the Convention. One of those aspects was the development of a global interoperable standard for the "biometric template based on a fingerprint printed as numbers in a bar code" that is required by the Convention. The Governing Body last November approved a plan that had been proposed by the Office following an informal meeting in September 2003 of Government experts, representatives of Shipowners and Seafarers, and relevant international organizations. In accordance with the plan, the Office has made arrangements for the "fast-track" preparation of a technical report containing the global interoperable standard concerned, which is reproduced in the appendices to the present paper. For the reasons given below, it is presented in two alternative versions, Appendix I, Finger pattern-based biometric profile for seafarers' identity documents, and Appendix II, Finger minutiae-based biometric profile for seafarers' identity documents.

2. The technical report contains the global interoperable standard required by the Convention. By following the standard in the technical report, all countries issuing the seafarers' identity document (SID) will be able to derive the same template from a seafarer's fingerprints and to embody the template in a bar code printed on the SID. Further, all countries visited by the seafarer will be able to read correctly the bar code so as to verify that the seafarer is indeed the holder of the SID. The Office can make this statement concerning interoperability with a high degree of certainty because of: (a) the quality of the technical report; (b) the expertise of the persons overseeing the preparation of the report; and (c) the evident appropriateness of the various steps to be taken under the standard.

3. Concerning the quality of the report, the enterprise that prepared it was highly recommended by a Government representative involved in the development of the present standard. The co-authors have both carried out various functions in the government

[1] GB.288/3/2.

concerned that are related to identity documents and biometrics. Their enterprise offers independent technical consultation in authentication technologies and is closely involved in international standards development for biometric systems, including the preparation of standards for endorsement by the International Organization for Standardization (ISO). In fact, the technical report has been prepared in such a way as to facilitate a proposal for ISO endorsement of the new standard in due course.

4. With respect to the oversight, the technical report takes into account the guidance and comments that were provided by numerous expert Government representatives before and during the preparation of the report and by ISO experts. The Office is very grateful, in particular, for the careful review of the drafts of the report that was kindly made by those technical experts.

5. The appropriateness of the various steps to be taken under the standard can be seen by the clear references in the technical report to the bases on which they were established. These bases are, in the first place, the overriding preconditions set out in the Convention itself, which are carefully analysed in section 5.1 of each of the versions of the technical report in the appendices to this paper. Other such bases are the technical standards of the International Civil Aviation Organization (ICAO), which are to be followed in accordance with the Convention, as well as the relevant technical standards prepared or at an advanced stage of preparation in the framework of the ISO. The creativity of the technical report therefore essentially resides in its assembly into a uniform whole of various components consisting of technical procedures that are already in existence and that are clearly the best suited to perform the functions required by the standard.

6. There is, however, one aspect on which there was a strong divergence of opinion among the experts consulted. It concerns the way in which the series of numbers in the template to be represented in the bar code is derived from the image of a fingerprint. There are two methods, which are both the subject of standards being finalized in the framework of the ISO: the *pattern*-based method, where the template is determined by the geometrical patterns made by the ridges on the finger; and the *minutiae*-based method, where the template is determined by the number and positions of the minutiae (breaks and points of bifurcation) that are found in those ridges. In view of the divergence of opinion, in December 2003, the Office sent a request for information (RFI) on the subject to the governments of all ILO member States as well as a questionnaire to enterprises known to be suppliers of relevant technology or devices. As of 11 February 2004, of the responses to the RFI received from governments, 28 responded to the specific question concerning the technology. Twelve have expressed a preference for *minutiae*-based templates (including two major labour-supplying countries), 13 have stated no technology preference, and three have stated a preference for the *pattern*-based method.

7. Because of the division of opinion, the technical report to this paper is submitted in two alternative versions: one (ILO SID-0001) incorporates the *pattern*-based technology (Appendix I) and the other (ILO SID-0002), the *minutiae*-based technology (Appendix II). In section 5.1.4 of each version, an explanation is given as to why the *pattern*-based was selected in preference to the *minutiae*-based (ILO SID-0001) or why the *minutiae*-based was selected in preference to the *pattern*-based (ILO SID-0002). For the reasons given below, it seems clear that the *pattern*-based method, which was in fact the one that had been recommended by the September 2003 meeting, referred to in paragraph 1 above, would better meet the requirements of the Convention. The *minutiae*-based method has the advantages of both greater familiarity to the governments using the standard and a greater potential for integration with other national systems using fingerprint technology, particularly with respect to the investigation of crimes.

8. From a technical point of view, both methods are well suited to an interoperable and efficient verification that the holder of the identity document is the seafarer to whom it was issued. However, there is a measure of uncertainty concerning one function that would need to be performed if the *minutiae*-based method were selected for the SID, as only a limited amount of information can be stored in the SID bar code. Experts generally agree that the information should relate to two fingerprints (so that if one finger is not available at the time of verification or the image from it is not sufficiently clear, reference can be made to the other fingerprint). The information obtained by following existing standards will always fit into the bar code if the *pattern*-based method is used. On the other hand, there will be cases where the number of minutiae on the fingers concerned will produce information exceeding the bar code capacity, where the *minutiae*-based method is followed. The simple solution is, in those cases, to reduce the number of minutiae to be taken into account and the annexed version ILO SID-0002 establishes an appropriate way of doing this (see section 5.1.3, second paragraph). However, because this "truncation" has not been the subject of a tested standard, one could not at this stage be sure that it would always result in the same template.

9. Indeed, more generally, at this point the *pattern*-based method offers greater reliability. In the case of both methods, the international standards are still in draft form (though at an advanced stage). Products complying with the *pattern*-based draft standard have been formally tested by independent third parties, while products claiming compliance with the *minutiae*-based draft standard have not. As indicated in responses to the questionnaire sent to vendors, once the international standard has been finalized and their client-base demands product compliance with the standard, the vendors of *minutiae*-based products could be expected to make corresponding changes to their products. However, as in the case of any technology update of this kind, independent testing of *minutiae*-based products (including the effects of the truncation needed for the SID template) will be required to ensure that the changes have not degraded performance of the individual products or introduced unanticipated system vulnerabilities.

10. Article 3, paragraph 8(c), of the Convention requires that "the equipment needed for the provision and verification of the biometric … is generally accessible to governments at low cost". Here, the *pattern*-based method appears to be slightly preferable, as it would work efficiently with an image of lower resolution than that required for the other method. Less expensive equipment could thus be used for acquiring the fingerprint image during the processes for the issuance of the SID and subsequent verification of the holder's identity. However, one government response indicated that the more expensive, optical sensors should be used for this purpose (though not required by the *pattern*-based biometric method) because in its opinion such equipment would be more durable in maritime environments. Another factor that could affect the cost of equipment arises from the fact that, while there are a number of known consultants, systems integrators and other equipment manufacturers that use the *pattern*-based technology, there are many more known suppliers of the *minutiae*-based technology with their own consultants, systems integrators, and other equipment manufacturers. However, prior to formal independent testing of products to demonstrate compliance with (and feasibility of) the draft international standard, purchasers of *minutiae*-based equipment may have to depend upon a restricted number of vendors (perhaps a single vendor).

11. There is a definite weakness with the *minutiae*-based method in relation to the requirement that "it shall not be possible to reconstitute [the biometric] from the template" (Article 3, paragraph 8(b)). There are publications concerning methods for developing artefacts that could counterfeit evidence of a person's fingerprint with the aid of the *minutiae*-based template. No similar publications have been identified in the case of the *pattern*-based method.

12. A government with *minutiae*-based systems should have no particular difficulty in using a *pattern*-based programme to produce and verify the fingerprint template (just as several completely different programmes can effectively run on the same computer). However, a *pattern*-based template could not be used for any search in databases in which fingerprints are only stored as *minutiae*-based templates, which may, in particular, be the case with national databases for criminal investigations. The use of the template for any purpose other than the verification of the seafarers' identity, however, is not in line with the intentions behind the Convention as reflected in several provisions, for example, paragraph 7 of Article 4: "Members shall ensure that the personal data on the electronic database shall not be used for any purpose other than verification of the seafarers' identity document".

13. Without prejudice therefore to the merits of the *minutiae*-based method from a general point of view, the Office concludes that the *pattern*-based method should be selected as the solution that better meets the requirements and intentions of the seafarers' identity documents Convention. In this connection, it should be noted that the aim of the Convention is not to put in place the best possible solution. Indeed, it was specifically decided not to embody the most effective solution of using a biometric image stored on a microchip. The aim is essentially to have a relatively inexpensive and acceptable biometric solution, adequate for use over the first five or more years of the Convention's life, that will effectively complement other personal data required by the Convention, such as signature and photograph, and to have this unprecedented solution in operation as a matter of urgency. Although the standard set out in the technical report still needs to be the subject of testing in a certification laboratory,[2] it is suggested that the Governing Body could now give its approval. In this way, potential ratifying Members will have a clear idea of the requirements in this respect. Any necessary adjustment of minor details could be made later.

14. ***In the light of the above, the Governing Body may wish:***

(a) to select the pattern-based option, as recommended by the Office, and approve document ILO SID-0001 (in Appendix I to this paper) as embodying the standard for the fingerprint template required under (k) of Annex I of the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185); or

(b) to select the minutiae-based option and approve document ILO SID-0002 (in Appendix II to this paper), as embodying the standard for the fingerprint template required under (k) of Annex I of the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185).

Geneva, 24 February 2004.

Point for decision: Paragraph 14.

[2] GB.288/3/2, para. 8.

Appendix I

Finger pattern-based biometric profile for seafarers' identity documents

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

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

Contents

Foreword

The International Labour Organization, established in 1919, is a specialized agency of the United Nations (UN). It is a tripartite organization, in which representatives of governments, employers and workers take part with equal status. In June 2003, the ILO adopted the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185). The revision of the earlier Convention of 1958 was prompted by discussions held in the International Maritime Organization (IMO), reviewing measures and procedures to prevent acts of terrorism that threaten the security of passengers and crews and the safety of ships. The new ILO Convention has now been communicated to the governments of ILO Members for their consideration with a view to ratification. It will become binding, as an international treaty, on all Members that ratify it.

The International Labour Office (the secretariat of the Organization) has commissioned the authors of this document to prepare a draft technical report to serve as a basis for a standard, to be later submitted to the International Organization for Standardization (ISO) with a view to endorsement, for an interoperable biometric template as required by Convention No. 185, covering fingerprint data capture, template generation, and bar code storage. The report should refer to the most appropriate print technology, reader technology, enrolment procedures, bar code format, biometric sensors/readers, database considerations and a global interoperable biometric template format. The report should also take into account database issues concerning quality and interoperability.

ISO and the International Electrotechnical Commission (IEC) 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.

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft international standards adopted by the joint technical committee are circulated to national bodies for voting.

This technical report was prepared by the International Labour Office (ILO) and can be submitted as a technical contribution to ISO/IEC JTC 1 SC37, Biometrics.

This report, ILO SID-0001, Finger pattern-based biometric profile for seafarers' identity documents, is organized into five sections; namely:

- section 1 – Scope;
- section 2 – Conformance;
- section 3 – References;
- section 4 – Terms and definitions;
- section 5 – SID biometric requirements.

Section 5, SID biometric requirements, is further organized into four subsections, namely:

- section 5.1 – SID finger pattern-based biometric requirements;
- section 5.2 – SID bar code and bar code reader requirements;
- section 5.3 – SID identity verification requirements;
- section 5.4 – SID database requirements.

0. Introduction

0.1. Rationale for document development

The International Labour Organization, established in 1919, is a specialized agency of the United Nations (UN). It is a tripartite organization in which representatives of governments, employers and workers take part with equal status. In the wake of the terrorist attacks of 11 September 2001, the International Labour Organization took steps to revise its 1958 Convention on seafarers' identity documents (also known as "seafarers' IDs" or "SIDs"), under an accelerated procedure. The new Convention, the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), which was adopted by the International Labour Conference in June 2003, introduced modern security features into the seafarers' ID to help to resolve the urgent question of seafarers being refused admission into the territory of countries visited by their ships for the purposes of shore leave and transit and transfer to join or change ships. One of those security features is a fingerprint biometric template, which shall be printed as numbers in a PDF417 bar code "conforming to a standard to be developed" (Convention No. 185, Annex I).

In a resolution adopted by the International Labour Conference in June 2003, the ILO Director-General was requested to take urgent measures "for the development by the appropriate institutions of a global interoperable standard" for the biometric template referred to above, particularly in cooperation with the International Civil Aviation Organization (ICAO). At a meeting held at the ILO in September 2003, which was attended by representatives of Governments, Shipowners, Seafarers, ICAO and ISO, it became clear that ICAO, which was proceeding with a recommendation for a different biometric solution (see below) as the standard for machine-readable passports, was not in a position to take an active part in the development of the template required by the new seafarers' ID. It was also noted that the urgent time frame required for the entry into operation of Convention No. 185 precluded a resort to the normal procedures for the development of such a template in the framework of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

The ILO has consequently commissioned this technical report to reflect the requirements generated by the seafarers' IDs Convention in 2003, which outlined high-level requirements for biometric-based personal identification of the international seafarer community. The authors submit this technical report, ILO SID-0001 rev. 05, in the form of a biometric profile defining the standard for generating and storing pattern-based fingerprint templates on the PDF417 bar code of the next-generation SID and in the Member's national electronic databases (international labour Convention No. 185, Annex I and Annex II, respectively). This biometric profile is organized in near-ISO-standard-compliant form that can be matured into a standard and then into a procurement document following international discussion and harmonization of the requirements.

0.2. Related efforts

Various studies, experiments, pilot programmes and products have been developed in recent years in attempts to expedite the inspection process at border management points. Many efforts will incorporate biometric technology into next-generation travel documents and international identification documents. The ILO drafted and approved Convention No. 185 to define requirements for the next-generation seafarers' IDs, which will incorporate biometric-based personal identification for the seafarer (document holder) and store biometric templates in a bar code printed on the SID.

Prior to 11 September 2001, the biometrics industry had initiated several standards development projects to facilitate the development of interoperable biometrics products and systems, as well as the interchange of biometrics data objects between products and systems and requirements for ensuring the integrity and privacy of biometric data.

- ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (BioAPI) (ISO/IEC JTC 1 SC37 N number 55, [1] dated 17 December 2002), which provides an application programming interface that assures that conforming products and systems can interoperate with each other. (This is also a final American National Standards Institute/International Committee for Information Technology Standards standard: ANSI/INCITS 358:2002 – Information technology – BioAPI specification).
- ISO/IEC CD 19785 – Information technology – Common biometric exchange formats framework (CBEFF) (ISO/IEC JTC1 SC37 N 208, dated 14 July 2003).
- ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003). (This is also a final ANSI/INCITS standard: ANSI/INCITS 377 – Finger pattern-based interchange format.)
- The International Civil Aviation Organization (ICAO) standard (document 9303) for machine-readable travel documents (MRTDs), commissioned by ISO/IEC JTC1 SC17.

  Note: The latest recommendation of ICAO is to include contactless smart card technology in next-generation travel documents and to include one or more biometrics (the facial biometric is required by the ICAO MRTD standard and either fingerprint or iris recognition systems could also be incorporated). While the ILO seafarers' ID is an identity document (and not a travel document), the ILO will attempt to follow the ICAO-proposed standard for next-generation MRTD where possible. It is important to note that the next-generation ILO seafarers' ID will use bar code technology to store biometric data (not the embedded chip technology recommended by ICAO's MRTD standard). This difference significantly impacts the SID biometric profile. While bar code storage is less expensive than embedded chip storage, there is significantly less storage capacity available on the SID PDF417 bar code than there is in ICAO-recommended embedded chip storage.

Because the next-generation ILO seafarers' IDs will use bar code technology to store biometric data and support the ILO's international interoperability requirements of the SID, this biometric profile defines the format for PDF417 bar code storage of fingerprint templates. Consequently, ISO/IEC 15438:2001 (PDF417 bar code symbology) and ISO/IEC FDIS 15415 (PDF417 bar code print quality) are fundamentally applicable to this biometric profile.

Together the standards ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003), and ICAO 9303, represent the foundation upon which the biometric capabilities of the seafarers' ID systems will be built. Other standards either already developed (such as ANSI/INCITS 358:2002 – Information technology – BioAPI specification) or being developed in parallel with this one, such as the ISO/IEC 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) will also be relevant as incorporated below.

0.3. Determination of the SID fingerprint biometric technology option

ILO Convention No. 185 requires that the SID be internationally interoperable. Therefore, the ILO had to choose between finger *image*, *minutiae*-, or *pattern*-based biometrics as the basis of procurement for the next-generation seafarer's ID. Two technical reports were prepared and ILO Members and relevant technical communities were surveyed to support the ILO's decision. This report, ILO SID-0001, represents the technical requirements for the finger pattern-based biometric option, which has been selected as the best fit solution for the ILO SID application requirements-based rationale given in section 5.1.3, Fingerprint template, of this technical report.

The ILO reserves the right to revisit this decision as international standards mature and technology options evolve to support ILO Convention No. 185.

[1] To review the referenced document ISO/IEC JTC 1 SC37 document number (N number), go to the www.jtcl.org web site, select subcommittee 37, search for documents, and enter the document number in the N number field.

1. Scope

This technical report, ILO SID-0001, Finger pattern-based biometric profile for seafarers' identity documents, gives guidelines for incorporation of pattern-based fingerprint biometric technology into the SID in accordance with the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185). Additional resources provided to the authors of this document included: (1) the functional brief for the biometric template prepared by the Informal Meeting on Biometrics for the SID held on 29-30 September 2003; (2) additional supporting material; (3) the technical consultation meeting in Geneva, 5-7 December 2003; and (4) advice of experts in the field.

Biometrics shall be used to increase the strength of the binding between the SID document and the seafarer who holds it.

The report is organized as follows. Conformance requirements for this biometric profile are organized in section 2. Technical references and definitions that pertain to this document are organized under sections 3 and 4, respectively. The biometric requirements for the SID are organized under section 5. There are four major subdivisions under section 5, namely:

- section 5.1 – SID finger pattern-based biometric requirements, which includes fingerprint enrolment, fingerprint capture, and the SID fingerprint template format to be incorporated into the next-generation seafarers' ID;
- section 5.2 – SID bar code requirements, which includes bar code format, printer technology and printing specifications, reader technology, and bar code physical characteristics;
- section 5.3 – SID identity verification requirements, which outlines the SID biometric identity verification procedure;
- section 5.4 – SID database requirements, which includes bar code database requirements and SID national electronic database requirements.

Annex A details the SID bar code format. Annex B details the SID pattern-based biometric data format. Annex C includes a copy of ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003). And, Annex D includes a copy of ISO/IEC 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).

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.

The following issues are outside of the scope of this technical report.

(1) The overall process of seafarer identification systems incorporating biometric technologies.

(2) Criteria for validation of individual seafarer's identities and of their professional titles.

(3) Criteria for SID issuance.

(4) Suitability of other than finger pattern-based biometric technologies to the seafarers' ID programme.

(5) Criteria for the "other security features" referred to in the introduction to Annex I of Convention No. 185.

(6) Marine environmental issues, including saline crystalline corrosion issues, are out of scope of this biometric profile, but should be addressed in SID procurement specifications.

(7) Application risk assessments.

2. Conformance

A biometric system conforms to this standard if it correctly performs all the mandatory capabilities defined in section 5, SID biometric requirements, in Annex A, SID pattern-based fingerprint bar code format, and in Annex B, SID bar code pattern-based fingerprint storage format.

Not all biometric technologies and features are appropriate for the seafarer ID based on the ILO's requirements and on the maturity of international standards for fingerprint biometric

technologies as of the date of this publication. This standard provides the requirements to enable international interoperability of the pattern-based fingerprint biometric components of next-generation seafarers' IDs.

3. References

This biometric profile is being developed prior to finalization of related draft standards. Any draft standard that is referenced in this section will list the SC37 document register number (N number) and the date of publication of the referenced draft. A copy of any referenced draft *conformative standard* (see section 3.1) will be included as an annex to this document. 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.

3.1. Conformative standards

(a) ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (BioAPI) (ISO/IEC JTC 1 SC37 N number 55 dated 17 December 2002). (This is also a final ANSI/INCITS standard: ANSI/INCITS 358-2002 – Information technology – BioAPI specification.)

(b) ANSI/NIST-ITL 1-2000 – Data format for the interchange of fingerprint information – Table 5.

(c) ISO/IEC FDIS 15415 – Information technology – Automatic identification and data capture techniques – Bar code print quality test specification – Two dimensional symbols.

(d) ISO/IEC 15438:2001 – Information technology – Automatic identification and data capture techniques – Bar code symbology specifications – PDF417.

(e) ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003). (This is also a final ANSI/INCITS standard: ANSI/INCITS 377 – Finger pattern-based interchange format.)

(f) ISO/IEC 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).

(g) ISO/IEC 8859-15:1999 – Information technology – 8-bit single-byte coded graphic character sets – Part 15: Latin alphabet No. 9.

(h) ISO 3166-1:1997 – Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

(i) ISO/IEC 9945-1:2003 – Information technology – Portable operating system interface (POSIX) – Part 1: Base definitions.

3.2. Informative references

(j) ICAO document 9303 – Machine-readable travel documents (Part 1, 5th edition, 2003; Part 3, 2nd edition 2002).

(k) ANSI/NIST-ITL-1-2000, Standard data format for the interchange of fingerprint, facial, and scar mark and tattoo (SMT) information.

(l) ISO/IEC 7810:2003 – Identification cards – Physical characteristics.

3.3. Additional standards and documentation to be developed or prioritized for use by the seafarer community

(m) SID application profile standard.

(n) SID performance and interoperability testing and reporting standard.

(o) An adequate and user-friendly guidance document for taking fingerprints to assist enrolment and verification personnel to produce consistently reliable results.

4. Terms and definitions

The authors have attempted to ensure that the terms, definitions, symbols and abbreviated terms of this technical report conform to the emerging standard for biometric vocabulary harmonization, being developed by Working Group 1 of ISO/IEC JTC 1 SC37. Specific relevant terms are defined below for the reader's convenience.

4.1. Terms and definitions

4.1.1. Application profile

Conforming subsets or combinations of base standards used to provide specific functions. Application profiles identify the use of particular options in base standards, and provide a basis between applications and interoperability of systems.

4.1.2. Biometric

Pertaining to the field of biometrics, used as an adjective.

Note: "Biometric" should no longer be used as a noun.

4.1.3. Biometric authentication/biometrically authenticate

The use of biometric verification or identification to validate the authenticity of a subject.

4.1.4. Biometric data block (BDB)

A block of data with a defined format that contains one or more biometric samples or biometric templates.

4.1.5. Biometric identification/biometrically identify

Associate a biometric sample with an entry in a biometric database by comparing the biometric sample with all previously stored processed biometric samples in the database and generating scores indicating the degree of similarity between the compared samples.

4.1.6. Biometric information record (BIR)

A data structure containing a BDB, information identifying the BDB format, and possibly further information such as whether the BDB is digitally signed or encrypted.

4.1.7. Biometric interchange data record (BIDR)

A data structure, corresponding to one person, that contains a BIR (see 4.1.6) plus other information specific to seafarer ID systems, applications or functions.

4.1.8. Biometric sample

Information obtained from a biometric device, either directly or after further processing.

4.1.9. Biometric verification/biometrically verify

Validate that a biometric sample matches the previously stored processed biometric sample associated with the subject's claimed identity by comparing the templates, generating a score and comparing the score with the threshold.

4.1.10. Biometrically enrol

The process of collecting one or more biometric samples from a subject and the subsequent preparation and storage of one or more processed biometric samples and associated data representing that subject's identity.

4.1.11. Country code

The numeric three-digit country code defined in ISO 3166-1.

4.1.12. Data integrity

A system property concerning physically stored data, such as that stored on a seafarer's ID or in a SID national electronic database, such that the data cannot be altered without such alteration being detected and tracked.

4.1.13. Data privacy

A system property concerning physically stored data, such as that stored on a seafarer's ID or in a SID national electronic database, such that the data cannot be accessed or processed except by people or applications that have the specific rights and technological capability to do so.

4.1.14. Global interoperability of SID biometric data

Global acceptance of the SID fingerprint biometric data block stored in the 2-D bar code printed on the SID for seafarer verification.

4.1.15. Null-terminated

Ending with a zero byte (0x00).

4.1.16. Real-time

Of or pertaining to a mode of computer operation in which the computer collects data, computes with it, and uses the results to control a process as it happens.

4.1.17. Seconds since the epoch (SSE)

Seconds since the epoch, in a 32-bit unsigned integer, of the day specified as defined in ISO/IEC 9945-1:2003 section 4.14. While any second of a specified day is allowed, if the actual second of the day is not known, the SID application will default to the first second of that day.

4.1.18. Shall

In accordance with legislative practice, the term "shall" indicates a mandatory practice.

4.1.19. Should

In accordance with legislative practice, the term "should" indicates a recommended practice that is not mandatory.

4.1.20. Text stream

A stream of character data using the ISO 8859-15:1999 Latin alphabet encoding.

5. SID biometric requirements

5.1. SID finger pattern-based biometric requirements

Two-finger pattern-based biometric templates of the seafarer to whom the document has been issued shall be printed as numbers in a bar code conforming to the standard outlined in this document. ILO Convention No. 185 has a set of preconditions that must be met by the resultant system, which are highlighted below with the compliance strategy assumed by the authors of this biometric profile.

- "The fingerprint can be captured without any invasion of privacy of the persons concerned, discomfort to them, risk to their health or offence against their dignity" (international labour Convention No. 185, Article 3, paragraph 8(a)).

  This requirement is addressed with the assumption that seafarers will not perceive fingerprint capture and verification to be an invasion of their privacy or an offence against their dignity. It also assumes that the implementation of biometric systems and bar code readers will be installed ergonomically such that no discomfort to the seafarer is imposed. It furthermore assumes that risk to the seafarers' health is assessed upon system implementation and checkout; and that the systems will be routinely sanitized to prevent the spread of germs via contact with system components, such that there is no greater health risk in using the fingerprint capture device than there would be in using a door knob, for example.

- "The biometric [data] shall itself be visible on the document and it shall not be possible to reconstitute it from the template or other representation" (international labour Convention No. 185, Article 3, paragraph 8(b)).

  This requirement presumes that it is sufficiently difficult to reconstitute from the biometric data that will be stored in the bar code either an actual fingerprint (understood as "fingerprint image") or a fraudulent device that could be used to misrepresent seafarer intent or presence. It also presumes that the biometric data shall be considered visible when the bar code in which fingerprint biometric data is stored is printed on the next-generation SID, and that the ILO's decision to employ finger pattern-based templates will obviate misuse of stored biometric data and consequent abuse of seafarer identities.

- "The equipment needed for the provision and verification of the biometric [sample] is user-friendly and is generally accessible to governments at low cost" (international labour Convention No. 185, Article 3, paragraph 8(c)).

  This presumes that the "user-friendly" requirement can and will be satisfied via biometric system ergonomics by implementers and system users. It also assumes that the ILO's selection of bar code storage for finger pattern-based biometric data, which require lower-resolution, less-costly fingerprint capture devices satisfies the requirement for "generally accessible to governments at low cost".

- "The equipment [used] for the verification of the biometric [sample] can be conveniently and reliably operated in ports and in other places, including on board ship, where verification of identity is normally carried out by the competent authorities" (international labour Convention No. 185, Article 3, paragraph 8(d)).

  This presumes that the biometric and card reading systems will be able to be reliably used on board ships, in ports, and other places, such that the systems are not considered unusually susceptible to the corrosive saline atmospheric environments found in these areas.

- "The system in which the biometric [authentication] is to be used (including the equipment, technologies and procedures for use) provides results that are uniform and reliable for the authentication of identity" (international labour Convention No. 185, Article 3, paragraph 8(e)).

  This presumes that "uniform" implies conforming to this technical report to ensure interoperability. It also presumes that commercial biometric systems satisfy reliable "authentication of identity" (understood "verification of identity") for the seafarer population that will be utilizing these systems.

5.1.1. Biometric enrolment procedure

This technical report does not address the entire ILO SID identity proofing procedure but focuses on the biometric enrolment portion of the procedure. A qualified issuing agent shall be required to enter the personalization information listed in Annex A into the enrolment system. A fingerprint should be captured from the index finger of each hand.[2] If the index fingerprint is missing or damaged to the extent that a reliable fingerprint either cannot be created or cannot be enrolled due to poor quality, a fingerprint from another finger or thumb will be captured such that operational consistency, operational efficiency and seafarer convenience are maximized. The standard presentation order of fingers for enrolment is given below:

- right index finger;
- left index finger;
- right thumb;
- left thumb;
- right middle finger;
- left middle finger;
- right ring finger;
- left ring finger;
- right little finger;
- left little finger.

The SID issuing agent shall specify which fingers were enrolled at the time of biometric enrolment and this information shall be recorded in the header of the biometric template to be stored on the SID bar code (see Annex B).

The system should either automatically incorporate a quality measure or provide a quality measure to enrolment personnel along with a minimum acceptable quality measure to ensure that good quality templates are generated (collected, captured). The best possible quality fingerprints should be enrolled and fingerprint templates should be stored to achieve reliable verification results. The seafarer shall be able to verify that his/her reference biometric data, which will be stored on his/her SID, can be used to support biometric verification, particularly at the place of issuance.

The biometric fingerprint system shall:

- provide on-screen prompts to both the SID issuing agent and the seafarer to support enrolment including procedural prompts, quality assessment and finger placement feedback;
- employ content and quality measures to ensure quality of captured templates; comparing the content and quality measures to the thresholds set to determine whether to prompt the seafarer to present either the same finger for re-enrolment or the next finger for enrolment;
- provide a measure indicating the quality of the acquired fingerprint template and visual feedback to the operator (SID issuing agent) and the enrolee (seafarer) of the fingerprint image;
- in the event that an acceptable template cannot be acquired by the biometric system for a given finger, allow the SID issuing agent the option of selecting another finger for enrolment;
- allow the seafarer to biometrically verify before the SID bar code is printed to ensure that the acquired template corresponds to the fingerprint enrolled and is operationally acceptable to the seafarer; providing a match indication (identity verified) if the matching score is above the

[2] Fingerprints from two fingers are acquired to improve the reliability and robustness of the system. The index finger is chosen for the primary fingerprint because in most cases the index finger is most easily placed on the fingerprint capture device, thus providing maximum convenience to the seafarer (Convention No. 185, Article 3, paragraph 8, precondition 1).

matching threshold to be used for verification (see 5.3.1 below) and a non-match indication (identity not verified) if the matching score is below the matching threshold;

- provide an indication of the number of successfully enrolled fingers;
- allow the SID issuing agent to review the textual data entered, modify as indicated, and print the SID bar code;
- support biometric verification of the seafarer using the printed SID as outlined in section 5.3.1.

5.1.2. Biometric enrolment documentation

User-friendly documentation shall be provided that instructs personnel how to perform the enrolment process to ensure that good quality fingerprints are enrolled and that good quality fingerprint templates are stored on the SID.

5.1.3. Fingerprint capture

During both enrolment and verification, the fingerprint capture device shall acquire finger pattern-based biometric templates that conform to table 1 in Annex A of ISO/IEC 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)[3] (see Annex D of this document for the entire draft standard) with a minimum fingerprint data capture quality level of 3[4] as qualified below:

- scan resolution: 98 pixels/cm (250 pixels/inch);
- pixel scale depth: 3 bits;
- dynamic range (grey levels): 8;
- certification: none.

The fingerprint capture device shall produce a 12.7 by 12.7 mm (0.5 by 0.5 inch) image of the fingerprint and the image shall be centred, preferably on the core of the fingerprint.

When the fingerprint image is transmitted to the template extraction algorithm, such as from the capture device to a computer, the data shall either be uncompressed or use lossless compression.

5.1.4. Fingerprint template

The algorithm shall extract a fingerprint template from the acquired fingerprint image in conformance with ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003). The fingerprint templates will be stored in the member State's national electronic database (Convention database) and in the PDF417 2-D bar code on the SID during the enrolment process and used for matching during the verification process.

A finger pattern-based template is stored for the following reasons:

1. Two seafarer fingerprint templates must be stored on the SID PDF417 bar code.

   (a) The memory required to store the fingerprint *image* of two fingers, whether encrypted or unencrypted, is beyond the storage capacity of the SID PDF417 2-D bar code.

[3] This working draft standard is currently a proposed standard that is under revision by ISO/IEC JTC 1 SC37 Working Group 3. We expect that the quality level 3 parameters will remain the same as the draft standard migrates to an approved standard. Nevertheless, the parameters specified in this document will take precedence for the SID.

[4] Fingerprint data capture quality level 3 is acceptable for images to be used to generate pattern-based fingerprint templates. Note that the fingerprint data capture quality is separate and distinct from the print image quality of the SID bar code.

(b) The size of finger *minutiae*-based templates is variable, a function of the number of minutiae detected on the finger.[5] According to a request for information (RFI) issued by the ILO to the biometric vendor community in December 2003, a typical minutiae template contains 50 to 60 minutiae. However, the maximum number of minutiae that can be stored within the memory constraints of the SID PDF417 bar code is 96 minutiae, or 48 minutiae per finger. As such, to store minutiae-based templates for two fingers on the SID bar code, the number of minutiae to be allowed and the overall size of the record to be stored must be constrained. Two options for constraining the size of minutiae-based templates were considered. The first option would list the maximum number of minutiae to be stored per fingerprint and specify the ILO SID method to prioritize minutiae for inclusion in the template. The second option would only list the maximum number of minutiae to be stored on the ILO SID PDF417 bar code. Neither option was deemed viable for the following reasons.

(i) Biometric vendor responses to the RFI issued by the ILO in December 2003 indicated that a consistent approach to template truncation does not exist. Consequently, the impact on individual biometric system performance of conforming to a prescribed method of truncation cannot be predicted or assured without thorough testing by a qualified laboratory.

(ii) Furthermore, if one vendor truncates their templates[6] to comply with the fixed size limitation of the ILO SID PDF417 bar code, the resultant impact on any vendor's biometric system performance cannot be predicted or assured without thorough testing by a qualified laboratory.

(iii) Test to assess the impacts of imposing a maximum template size and to assess the impact of imposing a specific method of prioritization of minutiae for inclusion or truncation is warranted prior to adoption of either strategy, but the ILO's timeline does not support a technology test phase prior to publication of this biometric profile.

(c) Finger *pattern*-based templates are of fixed size and two finger patterns can be stored within the memory constraints of the SID PDF417 bar code in accordance with ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003). (This document has been formalized as a standard under the title ANSI/INCITS 377 – Finger pattern-based interchange format.) This fixed-size pattern-based template strategy has been formally tested.

2. Compliant systems shall be generally accessible to governments at the lowest cost consistent with reliably achieving the purpose set out in Convention No. 185.

(a) In accordance with ISO/IEC 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), the image resolution required for *pattern*-based algorithms is less than that for *minutiae*-based algorithms (250 pixels per inch versus 500 pixels per inch). By using *pattern*-based algorithms, less expensive 250-pixel-per-inch fingerprint capture devices can be used.

3. Convention No. 185 states that it shall not be possible to reconstitute the biometric data from the template or other representation.

(a) Biometric data stored on the SID should not support misuse of the seafarers' biometric templates; in particular, it will be sufficiently difficult to reconstitute from the biometric

[5] ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003).

[6] While a proposal for standardized truncation of minutiae-based templates has recently been submitted to ISO for consideration, it is not clear that products are available to comply with this method and the ILO's timeline does not support a technology test phase prior to publication of this biometric profile.

data that will be stored in the bar code either an actual fingerprint (understood as "fingerprint image") or develop a fraudulent device that could provide false evidence of a seafarer's fingerprint.

(b) It may be possible to reconstitute a fingerprint image or develop a fraudulent device that could provide false evidence of a seafarer's fingerprint using data stored in *minutiae*-based and *image*-based fingerprint templates.[7] No published method employing data stored in *pattern*-based fingerprint templates to reconstitute a fingerprint image or develop a fraudulent device that could provide evidence of a seafarer's fingerprint has been identified.[8]

In accordance with ISO/IEC WD 19794-3 – Biometric data interchange formats – Part 3: Finger pattern data (ISO/IEC JTC 1 SC37 N 313, dated 3 October 2003), the ILO SID pattern-based biometric template has been specified in Annexes A, B and C. The seafarer's ID bar code data structure is summarized below:

- BioAPI-compliant header – 16 bytes;
- header for fingerprint pattern data – 32 bytes;
- two-finger pattern templates – 520 bytes;
- each finger pattern template shall have 224 cells: 14 cells per row by 16 rows. Each cell shall have 3-bit depth of angle, 3-bit depth of wavelength and 3-bit depth of phase offset;
- digital representation of data is described in Annex A – 120 bytes;
- total SID bar code size – 688 bytes.

5.2. SID bar code requirements

5.2.1. Bar code format

The SID bar code shall be formatted in accordance with Annex A. The pattern-based fingerprint SID bar code will contain 688 bytes of data and 64 data symbols for error correction level 5. The bar code shall contain the biometric template information and information that shall be printed on the face of the SID; specifically: the issuing authority, the optional personal identification number, the full name of the seafarer, the unique document number, the date of expiry of the document, the seafarers' nationality, their date, place of birth and gender, and the place and date of issue (see Annex A). The seafarers' biometric templates for two fingerprints shall be formatted in accordance with Annex B, which defines the 568 byte biometric data block referenced in Annex A. This 568 byte biometric data block plus the 120 byte header information outlined in Annex A comprises the total 688 byte SID bar code.

PDF417 2-D bar code technology shall be implemented for the following reasons:

- PDF417 symbols meet the data storage capacity requirements of this application;
- PDF417 symbols can be read with a 2-D scanner, or with standard CCD or laser scanners and special decoding software. Wand scanners, however, will not read symbols. This wide range of affordable, commercial bar code reader technology products will facilitate biometric verification of the seafarer community.

Dimensions and placement of the bar code shall conform to International Civil Aviation Organization (ICAO) specifications as contained in document 9303, Part 1 (5th edition, 2003), and document 9303, Part 3 (2nd edition, 2002), and outlined below for reader convenience:

[7] M. Bromba: "On the reconstruction of biometric raw data from template data", 9 July 2003. Download from page: http://www.bromba.com/knowhow/temppriv.htm.

[8] C.J. Hill: "Risk of masquerade arising from the storage of biometrics", BS thesis, Australian National University, 2001. Download from page: http://chris.fornax.net/biometrics.html.

- for SID booklets the maximum bar code size is 21.35 mm x 86.0 mm including quiet zones as specified in ICAO document 9303, Part 1 – Machine-readable passports – IV Technical specifications – Unique to machine-readable passports – Annex E (normative) Use of optional bar code(s) on machine-readable passports (MRP) data page;
- for SID cards the maximum bar code size is 27.8 mm x 85.6 mm [9] including quiet zones (see ICAO document 9303, Part 3 – Size 1 and size 2 machine-readable official travel documents – Appendix E (normative) to section IV – Use of the optional bar code(s) on the TD-1).

In addition, the SID bar code shall conform to the following:

- X-dimension: minimum width of symbol module is 0.170 mm (larger to fill card area, if possible, up to a maximum size of 0.175 mm);
- Y-dimension: minimum height of row is 0.511 mm (three times X-dimension, larger to fill card area, if possible, up to a maximum size of 0.525 mm);
- error correction level 5 as recommended in ISO/IEC 15438:2001, Annex E, and ICAO 9303 – Part 3 (2nd edition, 2002);
- number of data symbol columns = 16; [10]
- number of rows as necessary to contain the data (40 rows [11]).

5.2.2. Printer technology and printing specifications

The SID PDF417 bar code shall be printed in accordance with ISO/IEC 15438:2001. PDF417 2-D bar code symbols can be printed with most professional-grade thermal transfer, laser, and ink jet label printers. Next-generation SID bar code print quality shall conform to ISO/IEC FDIS 15415 – Bar code print quality test specification – Two dimensional symbols, with the designation of 3.0/05/660. The designation 3.0/05/660 refers to an overall symbol grade of 3.0 obtained using a 0.125 mm aperture at a wavelength of 660 nm.

SID bar codes shall be printed such that the resultant document is durable enough to withstand use as an identification document for seafarers.

Placement of the bar code printable area shall conform to ICAO specifications as contained in document 9303, Part 1 (5th edition, 2003), and document 9303, Part 3 (2nd edition, 2002).

5.2.3. Reader technology

Next-generation SID PDF417 symbols will be read with a 2-D scanner, or with standard CCD or laser scanners and special decoding software that read bar codes printed in compliance with sections 5.2.1 and 5.2.2 above. Wand scanners, however, will not read PDF417 symbols.

[9] This means that the next-generation SIDs in card form shall be size 1 MRTD and not size 2, as specified by ICAO 9303 – Part 3 (2nd edition, 2002).

[10] Mr. Sprague Ackley, an internationally recognized expert in PDF417 2-D bar code technology, states: “While it is a matter of argument exactly where 2-D imagers begin to have problems with PDF417 symbols with many columns, 25 data columns will almost certainly cause some 2-D imagers to fail.” The use of 16 data columns (20 overall) will enable the use of “2-D scanner” bar code reader technology with enough vertical room to fit the bar code/data on the SID.

[11] Derivation of the number of rows in the SID pattern-based bar code format follows. There are 688 bytes of SID data. Each codeword can store 1.2 bytes. Therefore, there are 688/1.2 = 574 codewords. Another 64 codewords are required for error correction codes at level 5 plus one codeword for total size of bar code. Therefore, there are 574 + 64 + 1 = 639 data symbols total on the SID bar code. There are 16 columns of data. Therefore, there are 639/16 = 40 rows required to store the SID bar code data.

5.2.4. Bar code physical characteristics

The "biometric template based on a fingerprint printed as numbers in a bar code" (international labour Convention No. 185, Annex I, paragraph 3(k)) "shall be protected by a laminate or overlay, or by applying an imaging technology and substrate material that provides an equivalent resistance to substitution of the portrait and other biographical data (international labour Convention No. 185, Annex I). This protection will also improve the durability of the bar code.

The "biometric shall itself be visible on the document" (international labour Convention No. 185, Article 3, paragraph 8(b)). This requirement is interpreted to mean that the biometric data shall be considered visible when the bar code in which fingerprint biometric data is stored is printed on the next-generation SID. The bar code shall be visible when printed on the SID. Furthermore, the seafarer shall be able to see a binary representation of the template embodied in the bar code and biometrically verify himself or herself using the SID as the source of reference data at issuance authority locations.

5.3. SID biometric verification requirements

5.3.1. Biometric verification procedure

A bar code reader shall scan the bar code on the SID and read the header and template information. The header shall specify which fingers' prints are stored in the bar code.

The system shall prompt the seafarer for the first finger template read from the bar code.

If the seafarer's finger corresponding to the first finger enrolled is unavailable, damaged, does not acquire, or does not achieve a matching score above the threshold value after three attempts, the system shall prompt the seafarer to place the second finger enrolled on the biometric capture device. If one live scan finger matches the corresponding templates stored on the bar code, the seafarer shall be successfully verified. If no live scan fingers match either of the corresponding templates stored on the bar code, the system shall return a failure to verify indication. If the system returns a failure to verify indication after the third attempt to verify both of the enrolled fingers, no more attempts using the same SID shall be permitted without the intervention of authorized verification personnel.

The biometric fingerprint system shall:

- retrieve the template from the SID PDF417 2-D bar code;
- provide on-screen prompts to both the SID verification authority and the seafarer to support verification, including procedural prompts, finger placement feedback and verification results;
- prompt the seafarer to place the appropriate finger on the image capture sensor;
- compare the acquired fingerprint image with the corresponding template stored in the bar code;
- provide a match indication (identity verified) if the matching score is above the matching threshold and provide a non-match indication (identity not verified) if the matching score is below the matching threshold;
- require verification personnel intervention if a seafarer fails to verify either enrolled finger after three attempts with each finger.

The fingerprint biometric system should:

- have the matching threshold set to a level that will be commensurate with a false finger match among the general public of less than 1 per cent and a false reject rate of less than 1 per cent;
- have content and quality measures that are commensurate with quality metrics for enrolment;
- optionally provide a measure indicating the quality of the acquired fingerprint template.

5.3.2. Biometric verification documentation

User-friendly documentation shall be provided that instructs personnel how to perform the verification process.

5.4. SID database requirements

5.4.1. Bar code database

"Seafarers shall have convenient access to machines enabling them to inspect any data concerning them that is not eye-readable. Such access shall be provided by or on behalf of the issuing authority" (international labour Convention No. 185, Article 3, paragraph 9). "Biometric template shall be based on a fingerprint printed as numbers in a bar code conforming to a standard" [this standard] (international labour Convention No. 185, Annex I).

The issuing authority shall provide seafarers access to machines enabling them to inspect the data stored in the SID PDF417 2-D bar code. The seafarer shall be able to verify that the fingerprint templates stored on their card match the fingers corresponding to the fingers enrolled. The non-fingerprint data shall be displayed in text format.

5.4.2. SID national electronic database

ILO Convention No. 185 has a set of requirements that must be met and a set of requirements that should be met by each Member with regard to the SID national electronic database that will impact the biometric system implementation and use. These requirements are highlighted below with the compliance strategy assumed by the authors of this biometric profile.

- "The details to be provided for each record in the electronic database to be maintained by each Member in accordance with Article 4, paragraphs 1, 2, 6 and 7, of this [International Labour Conference] Convention [185] shall be restricted to:

  1. Issuing authority named on the identity document.
  2. Full name of seafarer as written on the identity document.
  3. Unique document number of the identity document.
  4. Date of expiry or suspension or withdrawal of the identity document.
  5. Biometric template appearing on the identity document.
  6. Photograph (if stored in digital format).
  7. Details of all inquiries made concerning the seafarers' identity document." (International labour Convention No. 185, Annex II.)

  The national electronic database shall contain records of the seven items listed above for each seafarer that is issued a SID.

- "For the purposes of this Convention, appropriate restrictions shall be established to ensure that no data – in particular, photographs – are exchanged, unless a mechanism is in place to ensure that applicable data protection and privacy standards are adhered to." (International labour Convention No. 185, Article 4, paragraph 6.)

  Database access control mechanisms shall be implemented to protect seafarer information from unauthorized persons and unintended purposes.

- "The particulars of each item contained in [international labour Convention No. 185] Annex II are [shall be] entered in the database simultaneously with issuance of the SID." (International labour Convention No. 185, Annex III, Part A, paragraph 3(b)(i).)

  Member national electronic databases shall be updated with each SID issued in a timely manner.

- "Each Member shall ensure that a record of each seafarer's identity document issued, suspended or withdrawn by it is stored in an electronic database. The necessary measures shall be taken to secure the database from interference or unauthorized access." (International labour Convention No. 185, Article 4, paragraph 1.) "The seafarers' identity document shall be promptly withdrawn by the issuing State if it is ascertained that the seafarer no longer meets the conditions for its issue under this Convention." (International labour Convention No. 185, Article 7, paragraph 2.) "The issuing authority should draw up adequate procedures for protecting the database, including the restriction to specially authorized officials of

permission to access or make changes to an entry in the database once the entry has been confirmed by the official making it." (International labour Convention No. 185, Annex III, Part B, paragraph 4.2.2.)

Member national electronic databases shall implement an audit function that will log transactions including SID issuance, SID suspension, or SID withdrawal/cancellation. Database access control mechanisms shall be implemented to protect seafarer information from unauthorized persons and unintended purposes. Specially authorized officials within each Member's organization should have limited ability to make changes to the audit log; documentation of any such changes should be maintained by the Member.

- "Prompt action is [shall be] taken to update the database when an issued SID is suspended or withdrawn." (International labour Convention No. 185, Annex III, Part A, paragraph 3 (c).)

  Member national electronic databases shall be updated in a timely manner when SIDs are suspended or withdrawn.

- "An extension and/or renewal system has been [shall be] established to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost." (International labour Convention No. 185, Annex III, Part A, paragraph 3(d).) "The applicant should not be issued a SID for so long as he or she possesses another SID." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.)

  Members shall implement an extension and/or renewal system to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost. SID extension and/or renewal shall create a transaction in the national electronic database in a timely manner. In the event that a SID is rejected due to expiration, the national electronic database shall be checked to see if the SID has been extended or renewed. Seafarers' should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the seafarer. The biometric system shall support SID re-enrolment or reissuance.

- "An early renewal system should apply in circumstances where a seafarer is aware in advance that the period of service is such that he or she will be unable to make his or her application at the date of expiry or renewal." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.1.) "The applicant should not be issued a SID for so long as he or she possesses another SID." (International labour Convention No. 185, Annex III, Part B. paragraph 3.9.)

  Members shall implement an extension and/or renewal system to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID. The seafarer shall be able to instigate an extension and/or renewal at his or her convenience given that he or she will not be able to make his or her scheduled application for renewal. SID extension and/or renewal shall create a transaction in the national electronic database in a timely manner. In the event that a SID is rejected due to expiration, the national electronic database shall be checked to see if the SID has been extended or renewed. Seafarers' should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the seafarer. The biometric system shall support SID re-enrolment or reissuance.

- "A replacement system should apply in circumstances where a SID is lost. A suitable temporary document can be issued." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.3.) "The applicant should not be issued a SID for so long as he or she possesses another SID." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.)

  Members shall implement a replacement system to provide for circumstances where a seafarer loses his or her SID. SID replacement shall create a transaction in the national electronic database in real time. Seafarers should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the seafarer. The biometric system shall support SID re-enrolment or reissuance. The seafarer shall be able to instigate a replacement SID for any temporary document at his or her convenience. The temporary document will be surrendered. The national electronic database shall be updated to reflect the changes in a timely manner. Temporary documents shall only be issued by the issuing authority that issued the original SID.

- "The issuing authority should draw up adequate procedures for protecting the database, including a requirement for the regular creation of back-up copies of the database, to be stored on media held in a safe location away from the premises of the issuing authority." (International labour Convention No. 185, Annex III, Part B, paragraph 4.2.2.)

  Each Member's issuing authority should regularly create back-up copies of the national electronic database which should be stored on media held in a safe location away from the premises of the issuing authority.

- "Records of problems with respect to the reliability or security of the electronic database, including inquiries made to the database" should be maintained by the issuing authority within each Member. (International labour Convention No. 185, Annex III, Part B, paragraph 5.6.5.)

  Member national electronic databases shall implement an audit function that will log problems impacting the reliability or security of the electronic database (including inquiries made to the database).

Annex A

SID pattern-based fingerprint bar code format (normative)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pattern-based fingerprint SID bar code format (informative)

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

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

Annex B

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

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

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

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

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

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

1. The BioAPI header value shall be 16 bytes long and be 0x0000023801040101030 1nn0200000008 – 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

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

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

Date: 2003-09-08

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

Committee identification: ISO/IEC JTC 1/SC 37

Secretariat: ANSI

Biometric Data Interchange Formats — Part 3: Finger Pattern Data

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

Warning

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

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

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

Contents

Page

Foreword

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

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

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

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

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

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

— *Part 1:* Framework

— *Part 2:* Finger Minutiae Data

— *Part 3:* Finger Pattern Data

— *Part 4:* Finger Image Data

— *Part 5:* Face Image Data

— *Part 6:* Iris Image Data

— *Part 7:* Signature/Sign Data

Introduction

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

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

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

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

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

1 Scope

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

2 Conformance

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

3 Normative references

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

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

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

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

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

4 Terms and definitions

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

4.1 Biometric

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

4.2 Biometric Algorithm

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

4.3 Biometric Data

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

4.4 Biometric Sample

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

4.5 Biometric System

An automated system capable of:

capturing a biometric sample from an end user;

extracting biometric data from that sample;

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

deciding how well they match; and

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

4.6 Bit-Depth

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

4.7 Capture

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

4.8 Cell

Sub-portion of Finger Pattern (see 4.17).

4.9 Cell Structure

Structure used to represent the information contents of cell.

4.10 Cell Quality Group

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

4.11 Comparison

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

4.12 Crop

Remove the outer regions of an image.

4.13 Dimension

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

4.14 Down-sample

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

4.15 Encryption

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

4.16 Enrollment

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

4.17 Finger Pattern

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

4.18 Finger Pattern Interchange Data

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

4.19 Maximal Spatial Frequency

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

4.20 Packed Data Format

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

4.21 Pad

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

4.22 Raw Fingerprint Image

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

4.23 Reference Template

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

4.24 Resolution

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

4.25 Template Size

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

5 Finger Pattern Interchange Data

5.1 Overview

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

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

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

5.2 Step 1) Reduction in resolution

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

5.3 Step 2) Cellular Representation

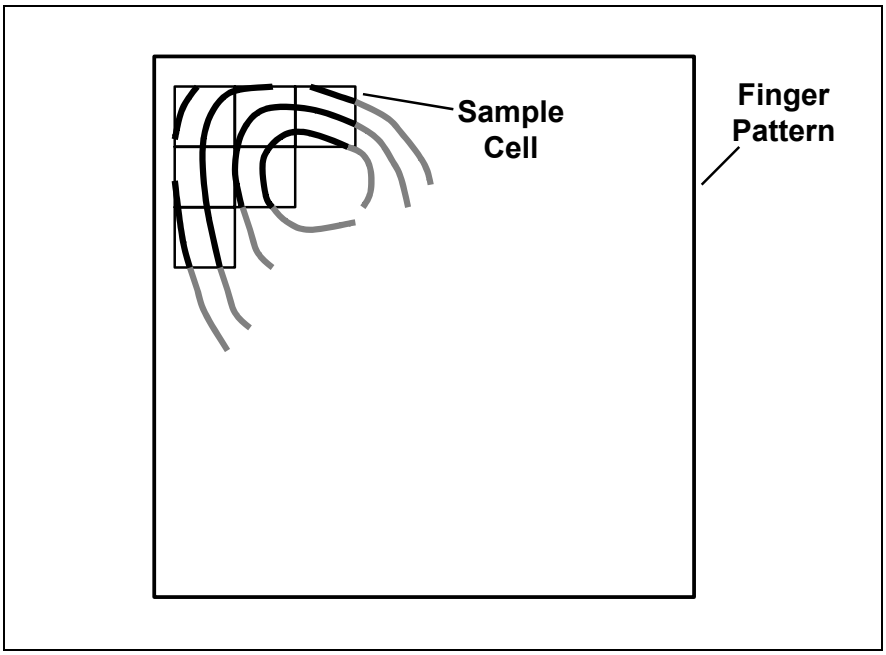


Figure 1. Diagram to illustrate Cellular Representation of Finger Pattern.

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

5.3.1 Cell Structure

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

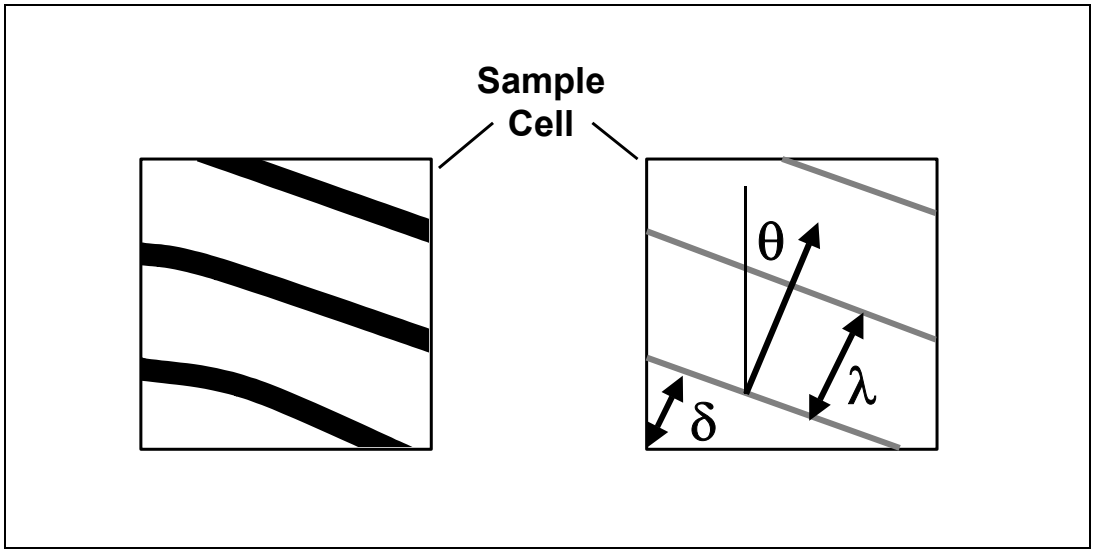


Figure 2. Cellular Representation of Finger Pattern.

The range of each of these parameters is given below:

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

λ: 0 to Maximal Spatial Frequency

δ: 0 to 360 degrees

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

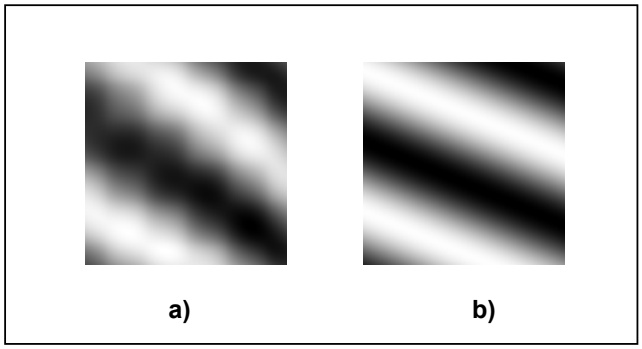


Figure 3. a) Example of the local finger pattern information in a cell, and b) the resulting cell structure chosen for representation.

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

5.4 Quality

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

6 Finger Pattern Data Record

6.1 Introduction

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

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

The BDB_PID shall be defined by CBEFF.

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

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

The organization of the record is as follows:

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

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

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

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

Extended data block - containing vendor-specific data.

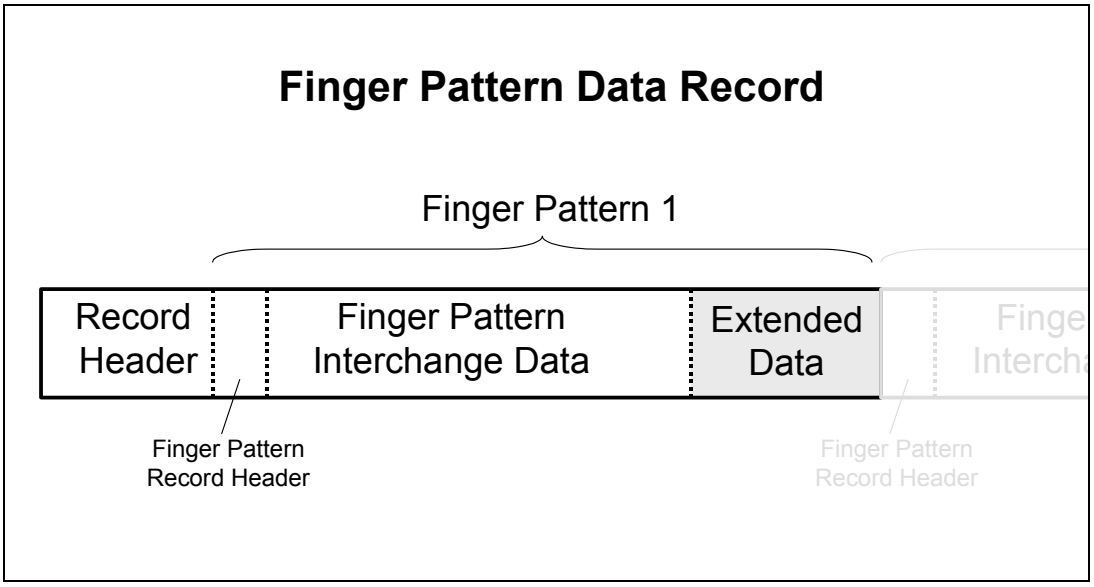


Figure 4. Diagram of Finger Pattern Data Record

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

6.2 Record Header

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

6.2.1 Format Identifier

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

6.2.2 Version Number

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

6.2.3 Length of Record

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

6.2.4 Capture Device ID

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

6.2.5 Number of Finger Patterns in Record

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

6.2.6 Resolution of Finger Pattern in x-direction

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

6.2.7 Resolution of Finger Pattern in y-direction

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

6.2.8 Number of Cells in x-direction

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

6.2.9 Number of Cells in y-direction

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

6.2.10 Number of Pixels in Cells in x-direction

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

6.2.11 Number of Pixels in Cells in y-direction

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

6.2.12 Cellular x-offset

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

6.2.13 Cellular y-offset

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

6.2.14 Bit-depth of Cell Structure Angle

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

6.2.15 Bit-depth of Cell Structure Wavelength

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

6.2.16 Bit-depth of Cell Structure Phase Offset

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

6.2.17 Bit-depth of Cell Structure Quality

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

6.2.18 Cell Quality Granularity

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

6.2.19 Reserved Bytes

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

6.3 Single Finger Pattern Record Format

6.3.1 Finger Pattern Record Header

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

6.3.1.1 Finger Location

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

Table 1 - Finger Location Codes

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

6.3.1.2 Impression type

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

Table 2 - Finger impression type

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

6.3.1.3 Number of Views in Finger Pattern

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

6.3.1.4 Finger Pattern Quality

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

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

6.3.1.5 Length of Data Block

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

6.3.2 Finger Pattern Data

6.3.2.1 Finger Pattern Interchange Data

6.3.2.1.1 View Number

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

6.3.2.1.2 Finger Pattern Cell Data

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

6.3.2.1.3 Cell Quality Data

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

6.3.2.2 Finger Pattern Extended Data

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

Table 3. Summary of Finger Pattern Data Record

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

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

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

Annex A (informative) - Finger Pattern Data Record Example

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

A.1 Reduction in Resolution

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

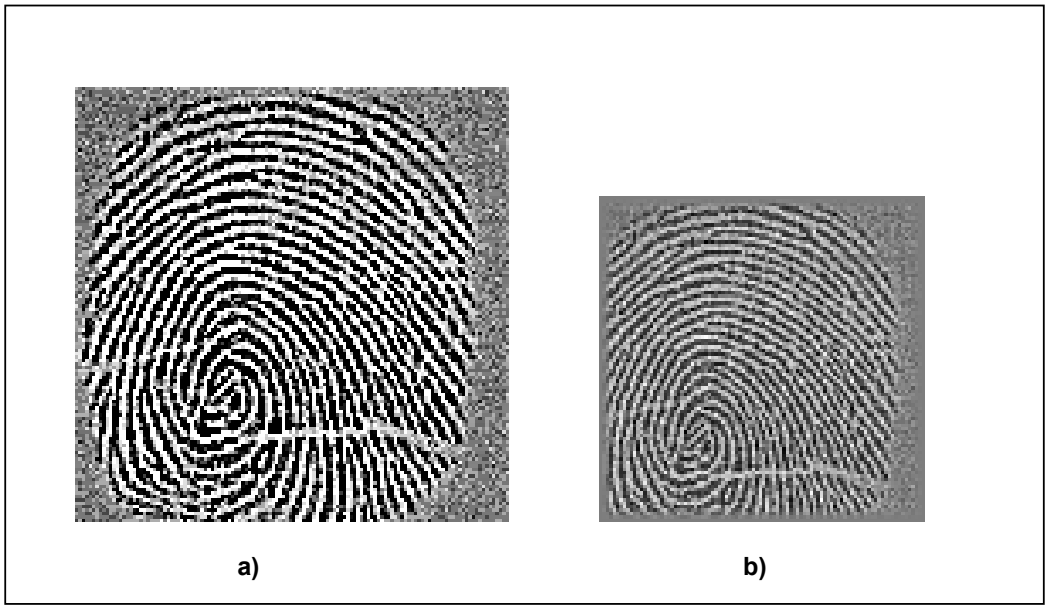


Figure 5. a) original 128x128 image sampled at 98.5 ppcm (250 ppi). b) resulting image after cropping image in a) to 120x120 pixels, and re-sampling image at 78.8 ppcm (200 ppi), to produce a 96x96 pixel dimensioned array.

A.2 Cellular Representation

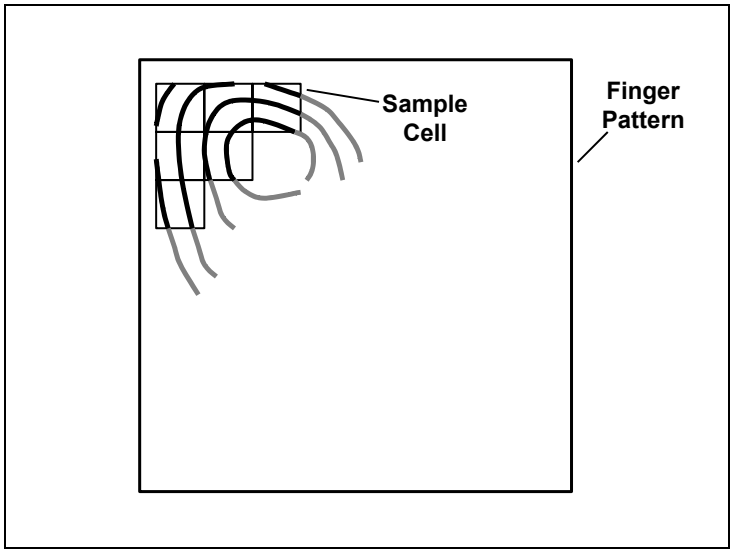


Figure 6. Diagram to illustrate Cellular Representation of Finger Pattern.

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

A.3 Cell Structure

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

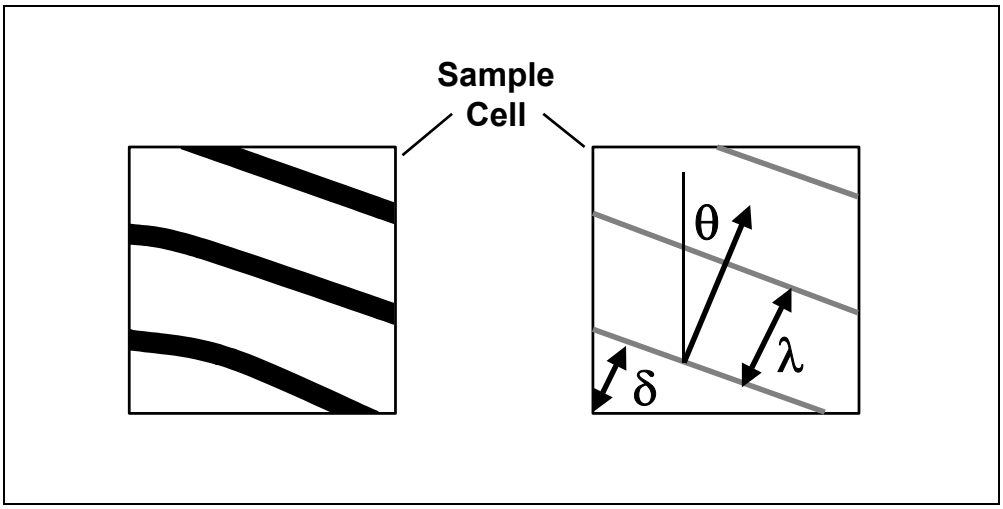


Figure 7. Cellular Representation of Finger Pattern.

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

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

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

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

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

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

A.4 Quality

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

A.5 Data Record

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

Table 4. Finger Pattern Data Record

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

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

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

Annex D

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

ISO/IEC JTC 1/SC 37 N341

2003-10-07

Replaces:

ISO/IEC JTC 1/SC 37
Biometrics

Document Type: Text for CD ballot or comment

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

Document Source: Project Editor

Project Number:

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

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

Action ID: LB

Due Date: 2004-01-07

Distribution:

Medium:

Disk Serial No:

No. of Pages: 31

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

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

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

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

ISO/IEC JTC 1/SC 37

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

Project: 1.37.19794.2

Introductory note:

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

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

ISO/IEC TC JTC 1/SC 37 N 341

Date: 2003-10-07

ISO/IEC CD 19794-4

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

Secretariat: ANSI

Biometric Data Interchange Formats – Part 4: Finger Image Data

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

Warning

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

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

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

Contents

Page

Foreword

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

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

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

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

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

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

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

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

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

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

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

— *Part 1: Framework*

— *Part 2: Finger Minutiae Data*

— *Part 3: Finger Pattern Data*

— *Part 4: Finger Image Data*

— *Part 5: Face Image Data*

— *Part 6: Iris Image Data*

— *Part 7: Signature/Sign Data*

Introduction

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

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

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

Biometric Data Interchange Formats – Part 4: Finger Image Data

1 Scope

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

2 Conformance

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

3 Normative references

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

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

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

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

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

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

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

4 Terms and definitions

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

4.1 biometric sample

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

4.2 capture

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

4.3 core

The approximate center of a fingerprint image area.

4.4 fingerprint image area

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

4.5 friction ridge

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

4.6 grayscale

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

4.7 image resolution

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

4.8 live capture

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

4.9 pixel:

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

4.10 plain fingerprint image

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

4.11 ppcm

Abbreviation for pixels per centimeter.

4.12 ppi

Abbreviation for pixels per inch.

4.13 ppmm

Abbreviation for pixels per millimeter.

4.14 rolled fingerprint image

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

4.15 scan resolution

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

4.16 transaction

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

4.17 valley

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

5 Data conventions

5.1 Byte and bit ordering

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

5.2 Scan sequence

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

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

6 Image requirements

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

6.1 Pixel aspect ratio

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

6.2 Pixel depth

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

6.3 Grayscale data

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

6.4 Dynamic range

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

6.5 Scan resolution

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

6.6 Image resolution

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

6.7 Fingerprint image location

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

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

7 Finger image record format

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

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

The organization of the record format is as follows:

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

7.1 General record header

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

Table 1 — General record header

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

7.1.1 Format Identifier

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

7.1.2 Version number

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

7.1.3 Record length

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

7.1.4 Capture device ID

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

7.1.5 Number of finger/palm images

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

7.1.6 Scale units

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

7.1.7 Scan resolution (horizontal)

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

7.1.8 Scan resolution (vertical)

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

7.1.9 Image resolution (horizontal)

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

7.1.10 Image resolution (vertical)

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

7.1.11 Pixel depth

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

7.1.12 Image Compression algorithm

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

7.1.13 Reserved

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

Table 2 — Compression algorithm codes

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

7.2 Finger record header

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

7.2.1 Length of finger/palm data block

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

7.2.2 Finger/palm position

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

Table 3 — Finger image header record

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

Table 4 — Finger position code and maximum size

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

7.2.3 Count of views

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

7.2.4 View number

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

7.2.5 Finger/palm image quality

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

Table 5 — Palm codes, areas, and dimensions

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

7.2.6 Impression type

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

7.2.7 Horizontal line length

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

Table 6 — Finger and palm impression types

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

7.2.8 Vertical line length

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

7.2.9 Finger/palm image data

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

Annex A

Bibliography -- Informative Reference

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

Annex B

Image acquisition requirements

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

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

Table 7 — Image acquisition settings levels

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

Annex C

IAFIS IMAGE QUALITY SPECIFICATIONS

Department of Justice

Federal Bureau of Investigation

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

ELECTRONIC FINGERPRINT TRANSMISSION SPECIFICATION

JANUARY 1999

Prepared By:

Federal Bureau of Investigation

Criminal Justice Information Services Division

935 Pennsylvania Avenue, N.W.

Washington, D.C. 20535

APPENDIX F

IAFIS IMAGE QUALITY SPECIFICATIONS

1.0 SCOPE AND PURPOSE

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

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

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

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

2.0 FINGERPRINT SCANNERS

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

2.1 Geometric Image Accuracy

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

D □ 0.0007, for 0 □ X □ 0.07

D □ 0.01X, for 0.07□ X □ 1.50

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

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

2.2 Modulation Transfer Function

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

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

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

(maximum - minimum) / (maximum + minimum)

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

MTF = representative image modulation / target modulation

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

---

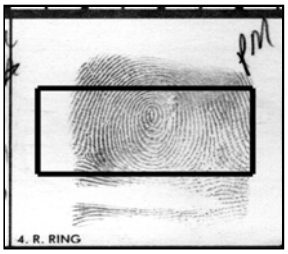
[1]Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

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

2.3 Signal-to-Noise Ratio

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

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



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

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

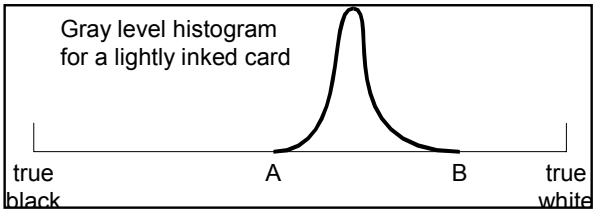
Note: The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level. Also, care should be taken, via direct visual or visual display observation, to avoid areas of dust, pinholes, scratches, or other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

2.4 Gray-Scale Range of Image Data

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

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

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



2.5 Gray-scale Linearity

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

2.6 Output Gray Level Uniformity

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

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

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

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

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

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

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

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

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

3.0 LATENT PRINT SCANNERS

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

3.1 Geometric Image Accuracy

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

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

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

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

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

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

3.2 Modulation Transfer Function

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

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

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

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

(maximum - minimum) / (maximum + minimum)

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

MTF = representative image modulation / target modulation

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

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

Appendix II

Finger minutiae-based biometric profile for seafarers' identity documents

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

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

Michael Crusoe
michael@authenti-corp.com
Phone: 480 889 6410

Contents

Foreword

The International Labour Organization, established in 1919, is a specialized agency of the United Nations (UN). It is a tripartite organization, in which representatives of governments, employers and workers take part with equal status. In June 2003, the ILO adopted the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185). The revision of the earlier Convention of 1958 was prompted by discussions held in the International Maritime Organization (IMO), reviewing measures and procedures to prevent acts of terrorism that threaten the security of passengers and crews and the safety of ships. The new ILO Convention has now been communicated to the governments of ILO Members for their consideration with a view to ratification. It will become binding, as an international treaty, on all Members that ratify it.

The International Labour Office (the secretariat of the Organization) has commissioned the authors of this document to prepare a draft technical report to serve as a basis for a standard, to be later submitted to the International Organization for Standardization (ISO) with a view to endorsement, for an interoperable biometric template as required by Convention No. 185, covering fingerprint data capture, template generation, and bar code storage. The report should refer to the most appropriate print technology, reader technology, enrolment procedures, bar code format, biometric sensors/readers, database considerations and a global interoperable biometric template format. The report should also take into account database issues concerning quality and interoperability.

ISO and the International Electrotechnical Commission (IEC) 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.

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft international standards adopted by the joint technical committee are circulated to national bodies for voting.

This report was prepared by the International Labour Office (ILO) and can be submitted as a technical contribution to ISO/IEC JTC 1 SC37, Biometrics.

This report, ILO SID-0002, Finger minutiae-based biometric profile for seafarers' identity documents, is organized into five sections; namely:

- section 1 – Scope;
- section 2 – Conformance;
- section 3 – References;
- section 4 – Terms and definitions;
- section 5 – SID biometric requirements.

Section 5, SID biometric requirements, is further organized into four subsections, namely:

- section 5.1 – SID finger minutiae-based biometric requirements;
- section 5.2 – SID bar code and bar code reader requirements;
- section 5.3 – SID identity verification requirements;
- section 5.4 – SID database requirements.

0. Introduction

0.1. Rationale for document development

The International Labour Organization, established in 1919, is a specialized agency of the United Nations (UN). It is a tripartite organization in which representatives of governments, employers and workers take part with equal status. In the wake of the terrorist attacks of 11 September 2001, the International Labour Organization took steps to revise its 1958 Convention on seafarers' identity documents (also known as "seafarers' IDs" or "SIDs"), under an accelerated procedure. The new Convention, the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), which was adopted by the International Labour Conference in June 2003, introduced modern security features into the seafarers' ID to help to resolve the urgent question of seafarers being refused admission into the territory of countries visited by their ships for the purposes of shore leave and transit and transfer to join or change ships. One of those security features is a fingerprint biometric template, which shall be printed as numbers in a PDF417 bar code "conforming to a standard to be developed" (Convention No. 185, Annex I).

In a resolution adopted by the International Labour Conference in June 2003, the ILO Director-General was requested to take urgent measures "for the development by the appropriate institutions of a global interoperable standard" for the biometric template referred to above, particularly in cooperation with the International Civil Aviation Organization (ICAO). At a meeting held at the ILO in September 2003, which was attended by representatives of Governments, Shipowners, Seafarers, ICAO and ISO, it became clear that ICAO, which was proceeding with a recommendation for a different biometric solution (see below) as the standard for machine-readable passports, was not in a position to take an active part in the development of the template required by the new seafarers' ID. It was also noted that the urgent time frame required for the entry into operation of Convention No. 185 precluded a resort to the normal procedures for the development of such a template in the framework of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

The ILO has consequently commissioned this technical report to reflect the requirements generated by the seafarers' IDs Convention in 2003, which outlined high-level requirements for biometric-based personal identification of the international seafarer community. The authors submit this technical report, ILO SID-0002 rev. 02, in the form of a biometric profile defining the standard for generating and storing minutiae-based fingerprint templates on the PDF417 2-D bar code of the next-generation SID and in the Member's national electronic databases (international labour Convention No. 185, Annex I and Annex II, respectively). This biometric profile is organized in near-ISO-standard-compliant form that can be matured into a standard and then into a procurement document following international discussion and harmonization of the requirements.

0.2. Related efforts

Various studies, experiments, pilot programmes and products have been developed in recent years in attempts to expedite the inspection process at border management points. Many efforts will incorporate biometric technology into next-generation travel documents and international identification documents. The ILO drafted and approved Convention No. 185 to define requirements for the next-generation seafarers' IDs, which will incorporate biometric-based personal identification for the seafarer (document holder) and store biometric templates in a bar code printed on the SID.

Prior to 11 September 2001, the biometrics industry had initiated several standards development projects to facilitate the development of interoperable biometrics products and systems, as well as the interchange of biometrics data objects between products and systems and requirements for ensuring the integrity and privacy of biometric data.

- ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (BioAPI) (ISO/IEC JTC 1 SC37 N number 55, [1] dated 17 December 2002), which provides an application programming interface that assures that conforming products and systems can interoperate with each other. (This is also a final American National Standards Institute/International Committee for Information Technology Standards standard: ANSI/INCITS 358:2002 – Information technology – BioAPI specification).
- ISO/IEC CD 19785 – Information technology – Common biometric exchange formats framework (CBEFF) (ISO/IEC JTC1 SC37 N 208, dated 14 July 2003).
- ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003).
- The International Civil Aviation Organization (ICAO) standard (document 9303) for machine-readable travel documents (MRTDs), commissioned by ISO/IEC JTC1 SC17.

  Note: The latest recommendation of ICAO is to include contactless smart card technology in next-generation travel documents and to include one or more biometrics (the facial biometric is required by the ICAO MRTD standard and either fingerprint or iris recognition systems could also be incorporated). While the ILO seafarers' ID is an identity document (and not a travel document), the ILO will attempt to follow the ICAO-proposed standard for next-generation MRTD where possible. It is important to note that the next-generation ILO seafarers' ID will use bar code technology to store biometric data (not the embedded chip technology recommended by ICAO's MRTD standard). This difference significantly impacts the SID biometric profile. While bar code storage is less expensive than embedded chip storage, there is significantly less storage capacity available on the SID PDF417 bar code than there is in ICAO-recommended embedded chip storage.

Because the next-generation ILO seafarers' IDs will use bar code technology to store biometric data and support the ILO's international interoperability requirements of the SID, this biometric profile defines the format for PDF417 bar code storage of fingerprint templates. Consequently, ISO/IEC 15438:2001 (PDF417 bar code symbology) and ISO/IEC FDIS 15415 (PDF417 bar code print quality) are fundamentally applicable to this biometric profile.

Together the standards ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC CD 19794-2 and ICAO 9303, represent the foundation upon which the biometric capabilities of the seafarers' ID systems will be built. Other standards either already developed (such as ANSI/INCITS 358:2002 – Information technology – BioAPI specification) or being developed in parallel with this one, such as the ISO/IEC 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) will also be relevant as incorporated below.

0.3. Determination of the SID fingerprint biometric technology option

ILO Convention No. 185 requires that the SID be internationally interoperable. Therefore, the ILO had to choose between finger *image*, *minutiae*-, or *pattern*-based biometrics as the basis of procurement for the next-generation seafarer's ID. Two technical reports were prepared and ILO Members and relevant technical communities were surveyed to support the ILO's decision. This report, ILO SID-0002, represents the technical requirements for the finger *minutiae*-based biometric option, which has not been selected as the best fit solution for the ILO SID application requirements. Rationale for selection of the finger *pattern*-based option is given in ILO SID-0001 rev. 05, Finger pattern-based biometric profile for seafarers' identity documents, section 5.1.3, Fingerprint template.

The ILO reserves the right to revisit this decision as international standards mature and technology options evolve to support ILO Convention No. 185.

[1] To review the referenced document ISO/IEC JTC 1 SC37 document number (N number), go to the www.jtcl.org web site, select subcommittee 37, search for documents, and enter the document number in the N number field.

1. Scope

This technical report, ILO SID-0002, Finger minutiae-based biometric profile for seafarers' identity documents, gives guidelines for incorporation of minutiae-based fingerprint biometric technology into the SID in accordance with the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185). Additional resources provided to the authors of this document included: (1) the functional brief for the biometric template prepared by the Informal Meeting on Biometrics for the SID held on 29-30 September 2003; (2) additional supporting material; (3) the technical consultation meeting in Geneva, 5-7 December 2003; and (4) advice of experts in the field.

Biometrics shall be used to increase the strength of the binding between the SID document and the seafarer who holds it.

The report is organized as follows. Conformance requirements for this biometric profile are organized in section 2. Technical references and definitions that pertain to this document are organized under sections 3 and 4, respectively. The biometric requirements for the SID are organized under section 5. There are four major subdivisions under section 5, namely:

- section 5.1 – SID finger minutiae-based biometric requirements, which includes fingerprint enrolment, fingerprint capture, and the SID fingerprint template format to be incorporated into the next-generation seafarers' ID;
- section 5.2 – SID bar code requirements, which includes bar code format, printer technology and printing specifications, reader technology, and bar code physical characteristics;
- section 5.3 – SID identity verification requirements, which outlines the SID biometric identity verification procedure;
- section 5.4 – SID database requirements, which includes bar code database requirements and SID national electronic database requirements.

Annex A details the SID bar code format. Annex B details the SID minutiae-based biometric data format. Annex C includes a copy of ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003). And, Annex D includes a copy of ISO/IEC 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).

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.

The following issues are outside of the scope of this technical report.

(1) The overall process of seafarer identification systems incorporating biometric technologies.

(2) Criteria for validation of individual seafarer's identities and of their professional titles.

(3) Criteria for SID issuance.

(4) Suitability of other than finger minutiae-based biometric technologies to the seafarers' ID programme.

(5) Criteria for the "other security features" referred to in the introduction to Annex I of Convention No. 185.

(6) Marine environmental issues, including saline crystalline corrosion issues, are out of scope of this biometric profile, but should be addressed in SID procurement specifications.

(7) Application risk assessments.

2. Conformance

A biometric system conforms to this standard if it correctly performs all the mandatory capabilities defined in section 5, SID biometric requirements, in Annex A, SID minutiae-based fingerprint bar code format, and in Annex B, SID bar code minutiae-based fingerprint storage format.

Not all biometric technologies and features are appropriate for the seafarer ID based on the ILO's requirements and on the maturity of international standards for fingerprint biometric technologies as of the date of this publication. This standard provides the requirements to enable international interoperability of the minutiae-based fingerprint biometric components of next-generation seafarers' IDs.

3. References

This biometric profile is being developed prior to finalization of related draft standards. Any draft standard that is referenced in this section will list the SC37 document register number (N number) and the date of publication of the referenced draft. A copy of any referenced draft *conformative standard* (see section 3.1) will be included as an annex to this document. 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.

3.1. Conformative standards

(a) ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (ISO/IEC JTC 1 SC37 N number 55 dated 17 December 2002).

(b) ANSI/NIST-ITL 1-2000 – Data format for the interchange of fingerprint information – Table 5.

(c) ISO/IEC FDIS 15415 – Information technology – Automatic identification and data capture techniques – Bar code print quality test specification – Two dimensional symbols.

(d) ISO/IEC 15438:2001 – Information technology – Automatic identification and data capture techniques – Bar code symbology specifications – PDF417.

(e) ISO/IEC CD 19794-3 – Biometric data interchange formats – Part 2: Finger minuitiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003).

(f) ISO/IEC 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).

(g) ISO/IEC 8859-15:1999 – Information technology – 8-bit single-byte coded graphic character sets – Part 15: Latin alphabet No. 9.

(h) ISO 3166-1:1997 – Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

(i) ISO/IEC 9945-1:2003 – Information technology – Portable operating system interface (POSIX) – Part 1: Base definitions.

3.2. Informative references

(j) ICAO document 9303 – Machine-readable travel documents (Part 1, 5th edition, 2003; Part 3, 2nd edition 2002).

(k) ANSI/NIST-ITL-1-2000, Standard data format for the interchange of fingerprint, facial, and scar mark and tattoo (SMT) information.

(l) ISO/IEC 7810:2003 – Identification cards – Physical characteristics.

3.3. Additional standards and documentation to be developed or prioritized for use by the seafarer community

(m) SID application profile standard.

(n) SID performance and interoperability testing and reporting standard.

(o) An adequate and user-friendly guidance document for taking fingerprints to assist enrolment and verification personnel to produce consistently reliable results.

4. Definitions

The authors have attempted to ensure that the terms, definitions, symbols and abbreviated terms of this technical report conform to the emerging standard for biometric vocabulary harmonization, being developed by Working Group 1 of ISO/IEC JTC 1 SC37. Specific relevant terms are defined below for the reader's convenience.

4.1. Terms and definitions

4.1.1. Application profile

Conforming subsets or combinations of base standards used to provide specific functions. Application profiles identify the use of particular options in base standards, and provide a basis between applications and interoperability of systems.

4.1.2. Biometric

Pertaining to the field of biometrics, used as an adjective.

Note: "Biometric" should no longer be used as a noun.

4.1.3. Biometric authentication/biometrically authenticate

The use of biometric verification or identification to validate the authenticity of a subject.

4.1.4. Biometric data block (BDB)

A block of data with a defined format that contains one or more biometric samples or biometric templates.

4.1.5. Biometric identification/biometrically identify

Associate a biometric sample with an entry in a biometric database by comparing the biometric sample with all previously stored processed biometric samples in the database and generating scores indicating the degree of similarity between the compared samples.

4.1.6. Biometric information record (BIR)

A data structure containing a BDB, information identifying the BDB format, and possibly further information such as whether the BDB is digitally signed or encrypted.

4.1.7. Biometric interchange data record (BIDR)

A data structure, corresponding to one person, that contains a BIR (see 4.1.6) plus other information specific to seafarer ID systems, applications or functions.

4.1.8. Biometric sample

Information obtained from a biometric device, either directly or after further processing.

4.1.9. Biometric verification/biometrically verify

Validate that a biometric sample matches the previously stored processed biometric sample associated with the subject's claimed identity by comparing the templates, generating a score and comparing the score with the threshold.

4.1.10. Biometrically enrol

The process of collecting one or more biometric samples from a subject and the subsequent preparation and storage of one or more processed biometric samples and associated data representing that subject's identity.

4.1.11. Country code

The numeric three-digit country code defined in ISO 3166-1.

4.1.12. Data integrity

A system property concerning physically stored data, such as that stored on a seafarer's ID or in a SID national electronic database, such that the data cannot be altered without such alteration being detected and tracked.

4.1.13. Data privacy

A system property concerning physically stored data, such as that stored on a seafarer's ID or in a SID national electronic database, such that the data cannot be accessed or processed except by people or applications that have the specific rights and technological capability to do so.

4.1.14. Global interoperability of SID biometric data

Global acceptance of the SID fingerprint biometric data block stored in the 2-D bar code printed on the SID for seafarer verification.

4.1.15. Null-terminated

Ending with a zero byte (0x00).

4.1.16. Real-time

Of or pertaining to a mode of computer operation in which the computer collects data, computes with it, and uses the results to control a process as it happens.

4.1.17. Seconds since the epoch (SSE)

Seconds since the epoch, in a 32-bit unsigned integer, of the day specified as defined in ISO/IEC 9945-1:2003 section 4.14. While any second of a specified day is allowed, if the actual second of the day is not known, the SID application will default to the first second of that day.

4.1.18. Shall

In accordance with legislative practice, the term "shall" indicates a mandatory practice.

4.1.19. Should

In accordance with legislative practice, the term "should" indicates a recommended practice that is not mandatory.

4.1.20. Text stream

A stream of character data using the ISO 8859-15:1999 Latin alphabet encoding.

5. SID biometric requirements

5.1. SID finger minutiae-based biometric requirements

Two-finger minutiae-based biometric templates of the seafarer to whom the document has been issued shall be printed as numbers in a bar code conforming to the standard outlined in this document. ILO Convention No. 185 has a set of preconditions that must be met by the resultant system, which are highlighted below with the compliance strategy assumed by the authors of this biometric profile.

- "The fingerprint can be captured without any invasion of privacy of the persons concerned, discomfort to them, risk to their health or offence against their dignity" (international labour Convention No. 185, Article 3, paragraph 8(a)).

  This requirement is addressed with the assumption that seafarers will not perceive fingerprint capture and verification to be an invasion of their privacy or an offence against their dignity. It also assumes that the implementation of biometric systems and bar code readers will be installed ergonomically such that no discomfort to the seafarer is imposed. It furthermore assumes that risk to the seafarers' health is assessed upon system implementation and checkout; and that the systems will be routinely sanitized to prevent the spread of germs via contact with system components, such that there is no greater health risk in using the fingerprint capture device than there would be in using a door knob, for example.

- "The biometric [data] shall itself be visible on the document and it shall not be possible to reconstitute it from the template or other representation" (international labour Convention No. 185, Article 3, paragraph 8(b)).

  This requirement presumes that it is sufficiently difficult to reconstitute from the biometric data that will be stored in the bar code either an actual fingerprint (understood as "fingerprint image") or a fraudulent device that could be used to misrepresent seafarer intent or presence. It also presumes that the biometric data shall be considered visible when the bar code in which fingerprint biometric data is stored is printed on the next-generation SID.

- "The equipment needed for the provision and verification of the biometric [sample] is user-friendly and is generally accessible to governments at low cost" (international labour Convention No. 185, Article 3, paragraph 8(c)).

  This presumes that the "user-friendly" requirement can and will be satisfied via biometric system ergonomics by implementers and system users. It also assumes that the ILO's selection of bar code storage for finger minutiae-based biometric data satisfies the requirement for "generally accessible to governments at low cost".

- "The equipment [used] for the verification of the biometric [sample] can be conveniently and reliably operated in ports and in other places, including on board ship, where verification of identity is normally carried out by the competent authorities" (international labour Convention No. 185, Article 3, paragraph 8(d)).

  This presumes that the biometric and card reading systems will be able to be reliably used on board ships, in ports, and other places, such that the systems are not considered unusually susceptible to the corrosive saline conditions found in these areas.

- "The system in which the biometric [authentication] is to be used (including the equipment, technologies and procedures for use) provides results that are uniform and reliable for the authentication of identity" (international labour Convention No. 185, Article 3, paragraph 8(e)).

  This presumes that "uniform" implies that the biometric system conforms to this technical report to ensure interoperability and that the biometric system will work equally well for the entire seafarer population. It also presumes that commercial biometric systems satisfy reliable "authentication of identity" (understood "verification of identity") for the seafarer population that will be utilizing these systems.

5.1.1. Biometric enrolment procedure

This technical report does not address the entire ILO SID identity proofing procedure but focuses on the biometric enrolment portion of the procedure. A qualified issuing agent shall be required to enter the personalization information listed in Annex A into the enrolment system. A fingerprint should be captured from the index finger of each hand.[2] If the index fingerprint is missing or damaged to the extent that a reliable fingerprint either cannot be created or cannot be enrolled due to poor quality, a fingerprint from another finger or thumb will be captured such that operational consistency, operational efficiency and seafarer convenience are maximized. The standard presentation order of fingers for enrolment is given below:

- right index finger;
- left index finger;
- right thumb;
- left thumb;
- right middle finger;
- left middle finger;
- right ring finger;
- left ring finger;
- right little finger;
- left little finger.

The SID issuing agent shall specify which fingers were enrolled at the time of biometric enrolment and this information shall be recorded in the header of the biometric template to be stored on the SID bar code (see Annex B).

The system should either automatically incorporate a quality measure or provide a quality measure to enrolment personnel along with a minimum acceptable quality measure to ensure that good quality templates are generated (collected, captured). The best possible quality fingerprints should be enrolled and fingerprint templates should be stored to achieve reliable verification results. The seafarer shall be able to verify that his/her reference biometric data, which will be stored on his/her SID, can be used to support biometric verification, particularly at the place of issuance.

The biometric fingerprint system shall:

- provide on-screen prompts to both the SID issuing agent and the seafarer to support enrolment including procedural prompts, quality assessment and finger placement feedback;
- employ content and quality measures to ensure quality of captured templates; comparing the content and quality measures to the thresholds set to determine whether to prompt the seafarer to present either the same finger for re-enrolment or the next finger for enrolment;
- provide a measure indicating the quality of the acquired fingerprint template and visual feedback to the operator (SID issuing agent) and the enrolee (seafarer) of the fingerprint image;
- in the event that an acceptable template cannot be acquired by the biometric system for a given finger, allow the SID issuing agent the option of selecting another finger for enrolment;
- allow the seafarer to biometrically verify before the SID bar code is printed to ensure that the acquired template corresponds to the fingerprint enrolled and is operationally acceptable to the seafarer; providing a match indication (identity verified) if the matching score is above the

[2] Fingerprints from two fingers are acquired to improve the reliability and robustness of the system. The index finger is chosen for the primary fingerprint because in most cases the index finger is most easily placed on the fingerprint capture device, thus providing maximum convenience to the seafarer (Convention No. 185, Article 3, paragraph 8, precondition 1).

matching threshold to be used for verification (see 5.3.1 below) and a non-match indication (identity not verified) if the matching score is below the matching threshold;

- provide an indication of the number of successfully enrolled fingers;
- allow the SID issuing agent to review the textual data entered, modify as indicated, and print the SID bar code;
- support biometric verification of the seafarer using the printed SID as outlined in section 5.3.1.

5.1.2. Biometric enrolment documentation

User-friendly documentation shall be provided that instructs personnel how to perform the enrolment process to ensure that good quality fingerprints are enrolled and that good quality fingerprint templates are stored.

5.1.3. Fingerprint capture

During enrolment, the fingerprint capture device shall acquire finger minutiae-based biometric templates that conform to table 1 in Annex A of ISO/IEC 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) [3] (see Annex D of this document for the entire draft standard) with a minimum fingerprint data capture quality level of 3 [4] as qualified below:

- scan resolution: 197 pixels/cm (500 pixels/inch);
- pixel scale depth: 8 bits;
- dynamic range (grey levels): 220;
- certification: EFTS/F.

The fingerprint capture device shall produce an image of the fingerprint and the image shall be centred, preferably on the core of the fingerprint. A maximum of 52 minutiae shall be included in each fingerprint template. "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 [5] of the minutiae set and before sorting into the order required by the card." [6]

When the fingerprint image is transmitted to the template extraction algorithm, such as from the capture device to a computer, the data shall either be uncompressed or use lossless compression.

5.1.4. Fingerprint template

The algorithm shall extract a fingerprint template from the acquired fingerprint image in conformance with ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003). The fingerprint templates will be stored in the member State's national electronic database (Convention database) and in the

[3] This working draft standard is currently a proposed standard that is under revision by ISO/IEC JTC 1 SC37 Working Group 3. We expect that the quality level 3 parameters will remain the same as the draft standard migrates to an approved standard. Nevertheless, the parameters specified in this document will take precedence for the SID.

[4] Fingerprint data capture quality level 3 is acceptable for images to be used to generate minutiae-based fingerprint templates. Note that the fingerprint data capture quality is separate and distinct from the print image quality of the SID bar code.

[5] The convex hull is the smallest shape (polygon) that encompasses a set of points.

[6] ISO/IEC CD 19794-2, dated 7 October 2003 (ISO/IEC JTC 1 SC37 N 340, para. 8.3.1).

PDF417 2-D bar code on the SID during the enrolment process and used for matching during the verification process.

A finger *minutiae*-based template will be prioritized for use by the ILO to facilitate searches of existing government databases as part of the identity proofing process prior to SID issuance. Many member countries that responded to the December 2003 ILO RFI indicated that they intend to use fingerprint data to search against existing government databases. [7] These government databases are typically International Automated Fingerprint Information Systems (IAFIS) databases, which are designed to facilitate searching by *minutiae* template-based systems.

- Convention No. 185, Article 3, paragraph 8(b), states "*the biometric [understood as 'fingerprint data stored in the PDF417 bar code'] shall itself be visible of the document* and it shall not be possible to reconstitute it [understood as 'fingerprint image'] from the template or other representation".

  Seafarer biometric data shall be stored in the PDF417 bar code that shall be visibly printed on the SID.

  The biometric data shall be two minutiae-based templates that will be formatted as directed in Annexes B and C of this report.

  The ILO will need to test the impact of imposing the fixed template defined in Annexes B and C. The tests to be defined should assess the impact of the fixed-size template on individual commercial solutions and on the aggregated impacts of multiple commercial solutions. To date, no formal testing has been done to ensure that compliance with ILO Convention No. 185 requirements will impose no degradation of biometric system performance.

- Convention No. 185, Article 3, paragraph 8(b), states "the biometric [understood as 'fingerprint data stored in the PDF417 bar code'] shall itself be visible of the document and *it shall not be possible to reconstitute it [understood as 'fingerprint image'] from the template or other representation*".

  Performance testing of minutiae-based biometric products will not only address the impact of the fixed-size template but will also be designed to ensure that it is significantly difficult to reconstitute a fingerprint image or develop a fraudulent device that could be used to misrepresent seafarer intent or presence using data stored in individual vendors' fixed-size minutiae-based finger templates. [8]

In accordance with ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003), the ILO SID minutiae-based biometric template has been specified in Annexes A, B and C. The seafarer's ID bar code data structure is summarized below:

- BioAPI-compliant header – 16 bytes;
- header for fingerprint minutiae-template data – 30 bytes;
- two-finger minutiae templates – up to 520 bytes; [9]

[7] The current draft of the minutiae data storage standard does not comply with the current IAFIS standard, or other AFIS standards, however they are based on the same principles and ideas. A simple conversion programme would be required to make use of the data for matching against member States' databases.

[8] M. Bromba: "On the reconstruction of biometric raw data from template data", 9 July 2003. Download from page: http://www.bromba.com/knowhow/temppriv.htm. C.J. Hill: "Risk of masquerade arising from the storage of biometrics", BS thesis, Australian National University, 2001. Download from page: http://chris.fornax.net/biometrics.html.

[9] Up to 52 minutiae per finger will be represented. In the event that a finger has more than 52 minutiae, truncation will conform to ISO/IEC CD 19794-2, dated 7 Oct. 2003 (ISO/IEC JTC 1 SC37 N 340, paragraph 8.3.1), which states "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,

- digital representation of data as described in Annex A – 120 bytes;
- total SID bar code size – up to 686 bytes.

5.2. SID bar code requirements

5.2.1. Bar code format

The SID bar code shall be formatted in accordance with Annex A. The minutiae-based fingerprint SID bar code will contain up to 686 bytes of data and 64 data symbols for error correction level 5. The bar code shall contain the biometric template information and information that shall be printed on the face of the SID; specifically: the issuing authority, the optional personal identification number, the full name of the seafarer, the unique document number, the date of expiry of the document, the seafarers' nationality, their date, place of birth and gender, and the place and date of issue (see Annex A). The seafarers' biometric templates for two fingerprints shall be formatted in accordance with Annex B, which defines the maximum 566-byte biometric data block referenced in Annex A. This maximum 566-byte biometric data block plus the 120-byte header information outlined in Annex A comprises the total maximum size of 686 bytes in the SID bar code.

PDF417 2-D bar code technology shall be implemented for the following reasons:

- PDF417 symbols meet the data storage capacity requirements of this application;
- PDF417 symbols can be read with a 2-D scanner, or with standard CCD or laser scanners and special decoding software. Wand scanners, however, will not read symbols. This wide range of affordable, commercial bar code reader technology products will facilitate biometric verification of the seafarer community.

Dimensions and placement of the bar code shall conform to International Civil Aviation Organization (ICAO) specifications as contained in document 9303, Part 1 (5th edition, 2003), and document 9303, Part 3 (2nd edition, 2002), and outlined below for reader convenience:

- for SID booklets the maximum bar code size is 21.35 mm x 86.0 mm including quiet zones as specified in ICAO document 9303, Part 1 – Machine-readable passports – IV Technical specifications – Unique to machine-readable passports – Annex E (normative) Use of optional bar code(s) on machine-readable passports (MRP) data page;
- for SID cards the maximum bar code size is 27.8 mm x 85.6 mm [10] including quiet zones (see ICAO document 9303, Part 3 – Size 1 and size 2 machine-readable official travel documents – Appendix E (normative) to section IV – Use of the optional bar code(s) on the TD-1).

In addition, the SID bar code shall conform to the following:

- X-dimension: minimum width of symbol module is 0.170 mm (larger to fill card area, if possible, up to a maximum size of 0.175 mm);
- Y-dimension: minimum height of row is 0.511 mm (three times X-dimension, larger to fill card area, if possible, up to a maximum size of 0.525 mm);
- error correction level 5 as recommended in ISO/IEC 15438:2001, Annex E, and ICAO 9303 – Part 3 (2nd edition, 2002);
- number of data symbol columns = 16; [11]

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".

[10] This means that the next-generation SIDs in card form shall be size 1 MRTD and not size 2, as specified by ICAO 9303 – Part 3 (2nd edition, 2002).

[11] Mr. Sprague Ackley, an internationally recognized expert in PDF417 2-D bar code technology states, "While it is a matter of argument exactly where 2-D imagers begin to have problems with

- number of rows as necessary to contain the data (40 rows [12]).

5.2.2. Printer technology and printing specifications

The SID PDF417 bar code shall be printed in accordance with ISO/IEC 15438:2001. PDF417 2-D bar code symbols can be printed with most professional-grade thermal transfer, laser, and ink jet label printers. Next-generation SID bar code print quality shall conform to ISO/IEC FDIS 15415 – Bar code print quality test specification – Two dimensional symbols, with the designation of 3.0/05/660. The designation 3.0/05/660 refers to an overall symbol grade of 3.0 obtained using a 0.125 mm aperture at a wavelength of 660 nm.

SID bar codes shall be printed such that the resultant document is durable enough to withstand use as an identification document for seafarers.

Placement of the bar code printable area shall conform to ICAO specifications as contained in document 9303, Part 1 (5th edition, 2003), and document 9303, Part 3 (2nd edition, 2002).

5.2.3. Reader technology

Next-generation SID PDF417 symbols will be read with a 2-D scanner, or with standard CCD or laser scanners and special decoding software that read bar codes printed in compliance with sections 5.2.1 and 5.2.2 above. Wand scanners, however, will not read PDF417 symbols.

5.2.4. Bar code physical characteristics

The "biometric template based on a fingerprint printed as numbers in a bar code" (international labour Convention No. 185, Annex I, paragraph 3(k)) "shall be protected by a laminate or overlay, or by applying an imaging technology and substrate material that provides an equivalent resistance to substitution of the portrait and other biographical data (international labour Convention No. 185, Annex I). This protection will also improve the durability of the bar code.

The "biometric shall itself be visible on the document" (international labour Convention No. 185, Article 3, paragraph 8(b)). This requirement is interpreted to mean that the biometric data shall be considered visible when the bar code in which fingerprint biometric data is stored is printed on the next-generation SID. The bar code shall be visible when printed on the SID. Furthermore, the seafarer shall be able to see a binary representation of the template embodied in the bar code and to biometrically verify himself or herself using the SID as the source of reference data at issuance authority locations.

5.3. SID biometric verification requirements

5.3.1. Biometric verification procedure

A bar code reader shall scan the bar code on the SID and read the header and template information. The header shall specify which fingers' prints are stored in the bar code.

The system shall prompt the seafarer for the first finger template read from the bar code. If the seafarer's finger corresponding to the first finger enrolled is unavailable, damaged, does not acquire, or does not achieve a matching score above the threshold value after three attempts, the system shall prompt the seafarer to place the second finger enrolled on the biometric capture device. If one live

PDF417 symbols with many columns, 25 data columns will almost certainly cause some 2-D imagers to fail". The use of 16 data columns (20 overall) will enable the use of "2-D scanner" bar code reader technology with enough vertical room to fit the bar code/data on the SID.

[12] Derivation of the number of rows in the SID minutiae-based bar code format follows. There are 686 bytes of SID data. Each codeword can store 1.2 bytes. Therefore, there are 686/1.2 = 572 codewords. Another 64 codewords are required for error correction codes at level 5 plus one codeword for total size of bar code. Therefore, there are 572 + 64 + 1 = 637 data symbols total on the SID bar code. There are 16 columns of data. Therefore, there are 637/16 = 40 rows required to store the SID bar code data.

scan finger matches the corresponding templates stored on the bar code, the seafarer shall be successfully verified. If no live scan fingers match either of the corresponding templates stored on the bar code, the system shall return a failure to verify indication. If the system returns a failure to verify indication after the third attempt to verify both of the enrolled fingers, no more attempts using the same SID shall be permitted without the intervention of authorized verification personnel.

The biometric fingerprint system shall:

- retrieve the template from the SID PDF417 2-D bar code;
- provide on-screen prompts to both the SID verification authority and the seafarer to support verification, including procedural prompts, finger placement feedback and verification results;
- prompt the seafarer to place the appropriate finger on the image capture sensor;
- compare the acquired fingerprint image with the corresponding template stored in the bar code;
- provide a match indication (identity verified) if the matching score is above the matching threshold and provide a non-match indication (identity not verified) if the matching score is below the matching threshold;
- require verification personnel intervention if a seafarer fails to verify either enrolled finger after three attempts with each finger.

The fingerprint biometric system should:

- have the matching threshold set to a level that will be commensurate with a false finger match among the general public of less than 1 per cent and a false reject rate of less than 1 per cent;
- have content and quality measures that are commensurate with quality metrics for enrolment;
- optionally provide a measure indicating the quality of the acquired fingerprint template.

5.3.2. Biometric verification documentation

User-friendly documentation shall be provided that instructs personnel how to perform the verification process.

5.4. SID database requirements

5.4.1. Bar code database

"Seafarers shall have convenient access to machines enabling them to inspect any data concerning them that is not eye-readable. Such access shall be provided by or on behalf of the issuing authority" (international labour Convention No. 185, Article 3, paragraph 9). "Biometric template shall be based on a fingerprint printed as numbers in a bar code conforming to a standard" [this standard] (international labour Convention No. 185, Annex I).

The issuing authority shall provide seafarers access to machines enabling them to inspect the data stored in the SID PDF417 2-D bar code. The seafarer shall be able to verify that the fingerprint templates stored on their card match the fingers corresponding to the fingers enrolled. The non-fingerprint data shall be displayed in text format.

5.4.2. SID national electronic database

ILO Convention No. 185 has a set of requirements that must be met and a set of requirements that should be met by each Member with regard to the SID national electronic database that will impact the biometric system implementation and use. These requirements are highlighted below with the compliance strategy assumed by the authors of this biometric profile.

- "The details to be provided for each record in the electronic database to be maintained by each Member in accordance with Article 4, paragraphs 1, 2, 6 and 7, of this [International Labour Conference] Convention [185] shall be restricted to:

  1. Issuing authority named on the identity document.

2. Full name of seafarer as written on the identity document.
3. Unique document number of the identity document.
4. Date of expiry or suspension or withdrawal of the identity document.
5. Biometric template appearing on the identity document.
6. Photograph (if stored in a digital format).
7. Details of all inquiries made concerning the seafarers' identity document." (International labour Convention No. 185, Annex II.)

The national electronic database shall contain records of the seven items listed above for each seafarer that is issued a SID.

- "For the purposes of this Convention, appropriate restrictions shall be established to ensure that no data – in particular, photographs – are exchanged, unless a mechanism is in place to ensure that applicable data protection and privacy standards are adhered to." (International labour Convention No. 185, Article 4, paragraph 6.)

  Database access control mechanisms shall be implemented to protect seafarer information from unauthorized persons and unintended purposes.

- "The particulars of each item contained in [international labour Convention No. 185] Annex II are [shall be] entered in the database simultaneously with issuance of the SID." (International labour Convention No. 185, Annex III, Part A, paragraph 3(b)(i).)

  Member national electronic databases shall be updated with each SID issued in a timely manner.

- "Each Member shall ensure that a record of each seafarer's identity document issued, suspended or withdrawn by it is stored in an electronic database. The necessary measures shall be taken to secure the database from interference or unauthorized access." (International labour Convention No. 185, Article 4, paragraph 1.) "The seafarers' identity document shall be promptly withdrawn by the issuing State if it is ascertained that the seafarer no longer meets the conditions for its issue under this Convention." (International labour Convention No. 185, Article 7, paragraph 2.) "The issuing authority should draw up adequate procedures for protecting the database, including the restriction to specially authorized officials of permission to access or make changes to an entry in the database once the entry has been confirmed by the official making it." (International labour Convention No. 185, Annex III, Part B, paragraph 4.2.2.)

  Member national electronic databases shall implement an audit function that will log transactions including SID issuance, SID suspension, or SID withdrawal/cancellation. Database access control mechanisms shall be implemented to protect seafarer information from unauthorized persons and unintended purposes. Specially authorized officials within each Member's organization should have limited ability to make changes to the audit log; documentation of any such changes should be maintained by the Member.

- "Prompt action is [shall be] taken to update the database when an issued SID is suspended or withdrawn." (International labour Convention No. 185, Annex III, Part A, paragraph 3 (c).)

  Member national electronic databases shall be updated in a timely manner when SIDs are suspended or withdrawn.

- "An extension and/or renewal system has been [shall be] established to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost." (International labour Convention No. 185, Annex III, Part A, paragraph 3(d).) "The applicant should not be issued a SID for so long as he or she possesses another SID." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.)

  Members shall implement an extension and/or renewal system to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID and in circumstances where the SID is lost. SID extension and/or renewal shall create a transaction in the national electronic database in a timely manner. In the event that a SID is rejected due to expiration, the national electronic database shall be checked to see if the SID has been extended or renewed. Seafarers' should only possess one SID at a time. A reissued SID should invalidate

any SID previously issued to the seafarer. The biometric system shall support SID re-enrolment or reissuance.

- "An early renewal system should apply in circumstances where a seafarer is aware in advance that the period of service is such that he or she will be unable to make his or her application at the date of expiry or renewal." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.1.) "The applicant should not be issued a SID for so long as he or she possesses another SID." (International labour Convention No. 185, Annex III, Part B. paragraph 3.9.)

  Members shall implement an extension and/or renewal system to provide for circumstances where a seafarer is in need of extension or renewal of his or her SID. The seafarer shall be able to instigate an extension and/or renewal at his or her convenience given that he or she will not be able to make his or her scheduled application for renewal. SID extension and/or renewal shall create a transaction in the national electronic database in a timely manner. In the event that a SID is rejected due to expiration, the national electronic database shall be checked to see if the SID has been extended or renewed. Seafarers' should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the seafarer. The biometric system shall support SID re-enrolment or reissuance.

- "A replacement system should apply in circumstances where a SID is lost. A suitable temporary document can be issued." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.3.) "The applicant should not be issued a SID for so long as he or she possesses another SID." (International labour Convention No. 185, Annex III, Part B, paragraph 3.9.)

  Members shall implement a replacement system to provide for circumstances where a seafarer loses his or her SID. SID replacement shall create a transaction in the national electronic database in real time. Seafarers should only possess one SID at a time. A reissued SID should invalidate any SID previously issued to the seafarer. The biometric system shall support SID re-enrolment or reissuance. The seafarer shall be able to instigate a replacement SID for any temporary document at his or her convenience. The temporary document will be surrendered. The national electronic database shall be updated to reflect the changes in a timely manner. Temporary documents shall only be issued by the issuing authority that issued the original SID.

- "The issuing authority should draw up adequate procedures for protecting the database, including a requirement for the regular creation of back-up copies of the database, to be stored on media held in a safe location away from the premises of the issuing authority." (International labour Convention No. 185, Annex III, Part B, paragraph 4.2.2.)

  Each Member's issuing authority should regularly create back-up copies of the national electronic database which should be stored on media held in a safe location away from the premises of the issuing authority.

- "Records of problems with respect to the reliability or security of the electronic database, including inquiries made to the database" should be maintained by the issuing authority within each Member. (International labour Convention No. 185, Annex III, Part B, paragraph 5.6.5.)

  Member national electronic databases shall implement an audit function that will log problems impacting the reliability or security of the electronic database (including inquiries made to the database).

Annex A

SID minutiae-based fingerprint bar code format (normative)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Minutiae-based fingerprint SID bar code format (informative)

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

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

Annex B

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

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

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

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

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

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

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

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

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

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

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

SID minutiae-based fingerprint bar code storage format

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

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

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

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

ISO/IEC JTC 1/SC 37 N340

2003-10-07

Replaces:

ISO/IEC JTC 1/SC 37
Biometrics

Document Type: Text for CD ballot or comment

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

Document Source: Project Editor

Project Number:

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

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

Action ID: LB

Due Date: 2004-01-07

Distribution:

Medium:

Disk Serial No:

No. of Pages: 44

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

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

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

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

ISO/IEC JTC 1/SC 37

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

Project: 1.37.19794.2

Introductory note:

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

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

ISO/IEC JTC 1/SC 37 N 340

Date: 2003-10-03

ISO/IEC CD 19794-2

ISO/IEC JTC 1/SC 37/WG 3

Secretariat: ANSI

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

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

Warning

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

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

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

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

Contents

Page

Foreword

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

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

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

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

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

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

— *Part 1: Framework*

— *Part 2: Finger Minutiae Data*

— *Part 3: Finger Pattern Data*

— *Part 4: Finger Image Data*

— *Part 5: Face Image Data*

— *Part 6: Iris Image Data*

— *Part 7: Signature/Sign Data*

Introduction

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

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

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

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

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

1 Scope

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

2 Conformance

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

3 Normative references

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

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

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

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

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

4 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.30
User
The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.

4.31
Valley
The area surrounding a friction ridge, which does not make contact with an incident surface under normal touch; the area of the finger between two friction ridges.

4.32
Valley Bifurcation
The point at which a valley splits into two valleys or, alternatively, where two separate valleys combine into one.

4.33
Verification / Verify
The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.

5 Symbols (and abbreviated terms)

The following abbreviations apply for the document:

BER	Basic Encoding Rules
BIT	Biometric Information Template
CBEFF	Common Biometric Exchange Formats Framework
DO	Data Object
FAR	False Acceptance Rate
FRR	False Rejection Rate
ICC	Integrated Circuit Card
RFU	Reserved for Future Use
TLV	Tag-Length-Value

6 Minutiae Extraction

This section defines the placement of minutiae on the fingerprint. Compatible minutiae extraction is required for interoperability between different finger matchers for the purposes of matching an individual against a previously collected and stored finger record. The interoperability is based on defining the finger minutiae extraction rules, record formats and card formats that are common to many finger matchers for acceptable matching accuracy, while allowing for extended data to be attached for use with equipment that is compatible with it.

6.1 Principle

Establishment of a common feature-based representation must rest on agreement on the fundamental notion for representing a fingerprint. Minutiae are points located at the places in the fingerprint image where friction ridges end or split into two ridges. Describing a fingerprint in terms of the location and direction of these ridge endings and bifurcations provides sufficient information to reliably determine whether two fingerprint records are from the same finger.

The specifications of minutia location and minutia direction described below accomplish this. See Figure 1 for an illustration of the definitions below.

6.2 Minutia Type

Each minutia point has a "type" associated with it. There are two major types of minutia: a "ridge ending" and a "ridge bifurcation" or split point. There are other types of "points of interest" in the friction ridges that occur much less frequently and are more difficult to define precisely. More complex types of minutiae are usually a

combination of the basic types defined above. This standard defines a category of “other” minutia for points that are not clearly a ridge ending or a bifurcation.

A ridge ending may — alternatively — be regarded as a valley bifurcation depending on the method to determine its position (see below). The format type of the biometric information template indicates the use of ridge endings or valley bifurcations.

6.3 Minutia Location

The minutia location is represented by its horizontal and vertical position. The minutiae determination strategy considered in this document relies on skeletons derived from a digital fingerprint image. The ridge skeleton is computed by thinning down the ridge area to single pixel wide lines. The valley skeleton is computed by thinning down the valley area to single pixel wide lines. If other methods are applied, they should approximate the skeleton method.

6.3.1 Coordinate System

The coordinate system used to express the minutia points of a fingerprint shall be a Cartesian coordinate system. Points shall be represented by their X and Y coordinates. The origin of the coordinate system shall be the upper left corner of the original image with X increasing to the right and Y increasing downward. Note that this is in agreement with most imaging and image processing use. When viewed on the finger, X increases from right to left as shown in Figure 1. All X and Y values are non-negative.

The X and Y coordinates of the minutia points shall be in pixel units, with the spatial resolution of a pixel given in the “X Resolution” and “Y Resolution” fields of the format. X and Y resolutions are stated separately.

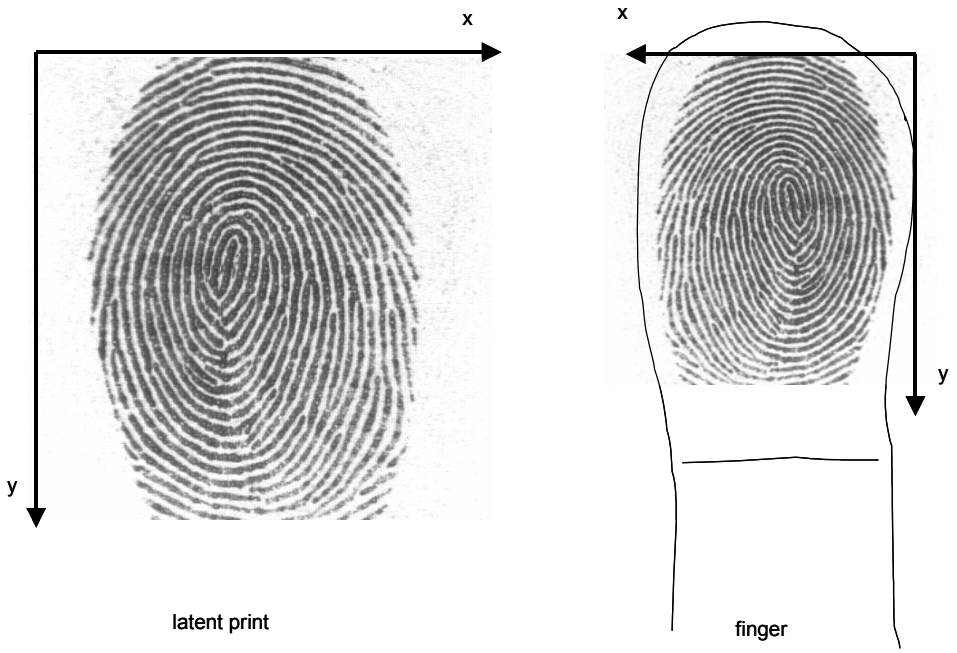


Figure 1 – Coordinate system

For the finger minutiae record format, the resolution of the coordinate system is specified in the record header, see 7.3.9 and 7.3.10. For the finger minutiae card format, the resolution of the X and Y coordinates of the minutia points shall be in metric units. The granularity is one bit per one hundredth of a millimeter in the normal format and one tenth of a millimeter in the compact format:

1 unit = 10^{-2} mm (normal format) or 10^{-1} mm (compact format).

6.3.2 Minutia Placement on a Ridge Ending (encoded as Valley Skeleton Bifurcation Point)

The minutia point for a ridge ending shall be defined as the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the valley area were thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia. In simpler terms, the point where the valley "Y"'s, or (equivalently) where the three legs of the thinned valley area intersect (see Fig. 2).

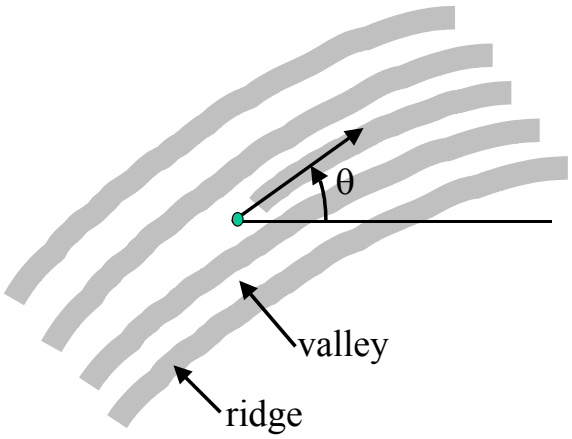


Figure 2 - Location and direction of a ridge ending (encoded as valley skeleton bifurcation point)

6.3.3 Minutiae Placement on a Ridge Bifurcation (encoded as a Ridge Skeleton Bifurcation Point)

The minutia point for a ridge bifurcation shall be defined as the point of forking of the medial skeleton of the ridge. If the ridge were thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia. In simpler terms, the point where the ridge "Y"'s, or (equivalently) where the three legs of the thinned ridge intersect (see Figure 3).

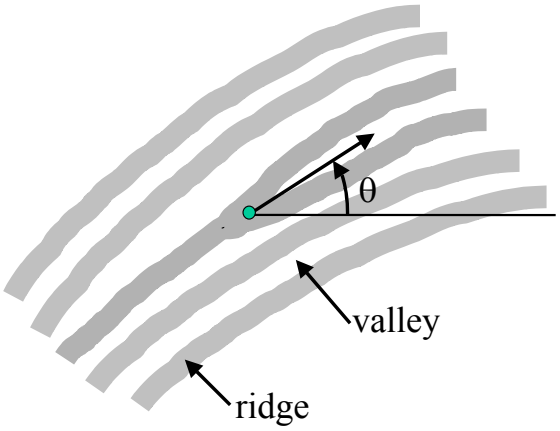


Figure 3 - Location and direction of a ridge bifurcation (encoded as ridge skeleton bifurcation point)

6.3.4 Minutiae Placement on a Ridge Skeleton Endpoint

The minutia point for a ridge skeleton endpoint shall be defined as the center point of the ending ridge. If the ridges in the digital fingerprint image were thinned down to a single-pixel-wide skeleton, the position of the minutia would be the coordinates of the skeleton point with only one neighbor pixel belonging to the skeleton (see Figure 4).

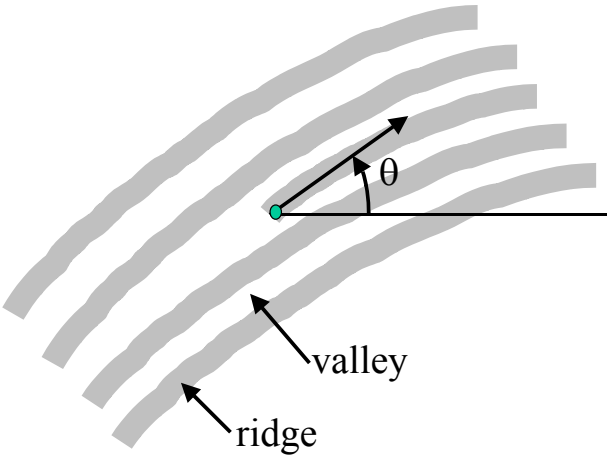


Figure 4 - Location and direction of a ridge skeleton endpoint

6.3.5 Minutiae Placement on Other Minutiae Types

For minutiae other than a bifurcation or ridge ending the placement and angle of direction shall be vendor defined.

6.3.6 Usage of the Minutiae Placement by the Record Formats and the Card Formats

The record formats use

- ridge ending and ridge bifurcation points.

The card formats use

- ridge ending and ridge bifurcation points, or

- valley skeleton bifurcation points and ridge bifurcation points

depending on the specific algorithms implemented. Typically, the card will request from a host system a minutiae record compatible with its matching algorithm. Both types of card formats are supported to avoid the on-card processing required to translate minutiae formats.

6.4 Minutia Direction

6.4.1 Angle Conventions

The minutiae angle is measured increasing counter-clockwise starting from the horizontal axis to the right.

In the record formats, the angle of a minutia is scaled to fit the granularity of 1.40625 (360/256) degrees per least significant bit.

The angle coding for the card formats depend on the normal size and the compact size format, see clause 8.1 and 8.2.

6.4.2 Minutia Direction of a Ridge Ending (encoded as Valley Skeleton Bifurcation Point)

A ridge ending (encoded as valley skeleton bifurcation point) has three arms of valleys meeting in one point. Two valleys encompass an acute angle. The tangent to the third valley lying opposite of the enclosed ridge defines the direction of a valley bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right (see Figure 2).

6.4.3 Minutia Direction of a Ridge Bifurcation (encoded as Ridge Skeleton Bifurcation Point)

A ridge bifurcation (encoded as ridge skeleton bifurcation point) has three arms of ridges meeting in one point. Two ridges encompass an acute angle. The tangent to the third ridge lying opposite of the enclosed valley defines the direction of a ridge bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right (see Figure 3).

6.4.4 Minutia Direction of a Ridge Skeleton End Point

The direction of a ridge skeleton endpoint is defined as the angle that the tangent to the ending ridge encompasses with the horizontal axis to the right (see Figure 4). Ridge skeleton end points are only used in

one type of the card formats, whereas in the other type ridge ending and ridge birfurcation is used as in the record format.

7 Finger Minutiae Record Format

7.1 Introduction

The minutiae record format shall be used to achieve interoperability between finger matchers providing a one-to-one verification. The minutia data shall be represented in a common format, containing both basic and extended data. With the exception of the Format Identifier and the Version number for the standard, which are null-terminated ASCII character strings, all data is represented in binary format. There are no record separators or field tags; fields are parsed by byte count.

7.2 Record Organization

The organization of the record is as follows:

- A fixed-length (24-byte) record header containing information about the overall record, including the number of fingers represented and the overall record length in bytes;
- A Single Finger record for each finger, consisting of:
- A fixed-length (4-byte) header containing information about the data for a single finger, including the number of minutiae;
- A series of fixed-length(6-byte) minutia point descriptions, including the position, type, angle and quality of the minutia point;
- One or more “extended” data areas for each finger, containing optional or vendor-specific information.

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

7.3 Record Header

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

7.3.1 Format Identifier

The Finger Minutiae Record shall begin with the three ASCII characters “FMR”. followed by a zero byte as a NULL string terminator.

7.3.2 Version Number

The version number for the version of this standard used in constructing the minutiae record shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major revision number and the third character will represent the minor revision number.

Upon approval of this specification, the version number shall be " 20" (an ASCII space followed by an ASCII '2' and an ASCII '0').

7.3.3 Length of Record

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

7.3.4 Capture Equipment Certifications

This field contains four bits used to indicate that the capture equipment used to capture the original fingerprint image was compliant with a standard certification method for such equipment. Currently, only the most significant bit is defined; if this bit is '1', the original capture equipment was certified to be compliant with the US Federal Bureau of Investigation's Image Quality Specifications, Appendix F. Three additional bits are reserved for future image quality certifications.

7.3.5 Capture Device ID

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

7.3.6 Size of Scanned Image in X direction

The size of the original image in pixels in the X direction shall be contained in two bytes.

7.3.7 Size of Scanned Image in Y direction

The size of the original image in pixels in the Y direction shall be contained in two bytes.

7.3.8 X (horizontal) resolution

The resolution of the minutiae coordinate system shall be recorded in two bytes having the units of pixels per centimeter. The value of the sensor X resolution shall not be zero.

7.3.9 Y (vertical) resolution

The resolution of the minutiae coordinate system shall be recorded in two bytes having the units of pixels per centimeter. The value of the sensor Y resolution shall not be zero.

7.3.10 Number Of Fingers

The number of fingers contained in the minutiae record shall be recorded in one byte.

7.3.11 View Number

If more than one finger minutiae record in a general record is from the same finger, each minutiae record shall have a unique view number. The combination of finger location and view number shall uniquely identify a particular minutiae record within a general record. Multiple finger minutiae records from the same finger shall be numbered with increasing view numbers, beginning with zero. Where only one finger minutiae record is taken from each finger, this field shall be set to 0.

7.4 Single Finger Record Format

7.4.1 Finger Header

A finger header shall start each section of finger data providing information for that finger. There shall be one finger header for each finger contained in the finger minutiae record. The finger header will occupy a total of four bytes as described below. Note that it is permissible for more than one finger record to represent the same finger, with (presumably) different data, perhaps in the private area.

7.4.1.1 Finger Position

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

Table 1 - Finger Position Codes

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

7.4.1.2 Impression Type

The impression type of the finger images that the minutiae data was derived from shall be recorded in one byte. The codes for this byte are shown in Table 2. These codes are compatible with Table 4 of ANSI/NIST-ITL 1-2000, “Data Format for the Interchange of Fingerprint Information”, with the addition of the “swipe” type. The “swipe” type identifies data records derived from image streams generated by sliding the finger across a small sensor. Only codes 0 through 3 and 8 shall be used; the “latent” codes are not relevant for this standard.

Table 2 - Impression Type Codes

Description	Code
Live-scan plain	0
Live-scan rolled	1
Nonlive-scan plain	2
Nonlive-scan rolled	3

Latent impression	*4*
Latent tracing	*5*
Latent photo	*6*
Latent lift	*7*
Swipe	8

7.4.1.3 Finger Quality

The quality of the overall finger minutiae data shall be between 0 and 100 and recorded in one byte. This quality number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutia record. A value of 0 shall represent the lowest possible quality and the value 100 shall represent the higher possible quality. The numeric values in this field will be set in accordance with the general guidelines contained in Section 2.1.42 of ANSI/INCITS 358-2002, "BioAPI H-Level Specification Version 1.1". The matcher may use this value to determine its certainty of verification.

7.4.1.4 Number of Minutiae

The number of minutiae recorded for the finger shall be recorded in one byte.

7.4.2 Finger Minutiae Data

The finger minutiae data for a single finger shall be recorded in blocks of six bytes per minutia point. The order of the minutiae is not specified.

7.4.2.1 Minutiae Type

The type of minutiae will be recorded in the first two bits of the upper byte of the X coordinate. There will be two bits reserved at the beginning of the upper byte of the Y coordinate for future use. The bits "00" will represent a minutia of "other" type, "01" will represent a ridge ending and "10" will represent a bifurcation.

7.4.2.2 Minutiae Position

The X coordinate of the minutia shall be recorded in the rest of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header. Note that position information shall be present for each minutia point, regardless of type, although position for minutiae of type "other" is vendor defined.

7.4.2.3 Minutiae Angle

The angle of the minutia shall be recorded in one byte in units of 1.40625 (360/256) degrees. The value shall be a non-negative value between 0 and 255, inclusive. For example, an angle value of 16 represents 22.5 degrees. Note that angle information shall be present for each minutia point, regardless of type, although angle for minutiae of type "other" is vendor defined.

7.4.2.4 Minutiae Quality

The quality of each minutia shall be recorded in one byte. The quality figure shall range from 100 as a maximum to 1 as a minimum. In interoperable use, only the relative values of minutiae quality values is meaningful; there is no guaranteed relationship between minutiae quality values assigned by different equipment suppliers. Any equipment that does not supply quality information for individual minutia points shall set all quality values to 0.

7.5 Extended Data

The extended data section of the finger minutiae record is open to placing additional data that may be used by the matching equipment. The size of this section shall be kept as small as possible, augmenting the data stored in the standard minutiae section. The extended data for each finger shall immediately follow the standard minutiae data. More than one extended data area may be present for each finger. In this case, the length of data fields may be used to index through the fields, relative to the overall length of record field in the record header.

While the extended data area allows for inclusion of proprietary data within the minutiae format, this is not intended to allow for alternate representations of data that can be represented in open manner as defined in this standard. In particular, ridge count data and core and delta information shall not be represented in proprietary manner to the exclusion of the publicly defined formats in this standard. Additional ridge count or core and delta information may be placed in a proprietary extended data area if the standard fields defined below are also populated. The intention of this standard is to provide interoperability.

7.5.1 Common Extended Data Fields

All records shall contain at least the type identification code (Section 7.5.1.1). If this code is all zeroes (0x0000 hexadecimal), then there is no extended data and the length of data and data areas (Sections 7.5.1.2 and 6.5.1.3) shall not be present.

7.5.1.1 Type Identification Code

The type identification code shall be recorded in two bytes, and shall distinguish the format of the extended data area (as defined by the Vendor specified by the PID code in the CBEFF header). A value of zero in both bytes shall indicate that there is no following extended data. A value of zero in the first byte, followed by a non-zero value in the second byte, shall indicate that the extended data section has a format defined in this standard. A non-zero value in the first byte shall indicate a vendor specified format, with a code maintained by the vendor. Refer to Table 3 for a summary of the type identification codes.

Table 3 - Extended Data Area Type Codes

First byte	Second byte	Identification
0x00	0x00	no extended data
0x00	0x01	ridge count data (Section 7.5.2)
0x00	0x02	core and delta data (Section 7.5.3)
0x00	0x03	zonal quality data (Section 7.5.4)
0x00	0x04-0xFF	reserved
0x01-0xFF	0x00	reserved
0x01-0xFF	0x01-0xFF	vendor-defined extended data

7.5.1.2 Length of Data

The length of the extended data section, including the vendor identification and length of data fields, shall be recorded in two bytes. This value is used to skip to the next finger minutiae data if the matcher cannot decode and use this data. If the type identification (field 7.5.1.1) for the private area is zero, indicating no private data, this field shall not be present.

7.5.1.3 Data Section

The data field of the extended data is defined by the equipment that is generating the finger minutiae record, or by common extended data formats contained in this standard; see section 6.5.2. If the type identification (field 7.5.1.1) for the private area is zero, indicating no private data, this field shall not be present.

7.5.2 Ridge Count Data Format

If the extended data area type code is 0x0001, the extended data area contains ridge count information. This format is provided to contain optional information about the number of fingerprint ridges between pairs of minutiae points. Each ridge count is associated with a pair of minutiae points contained in the minutiae data area defined in section 6.4.2; no ridge information may be contained that is associated with minutiae not included in the corresponding minutiae area. Ridge counts shall not include the ridges represented by either of the associated minutiae points. Refer to Figure 5 for clarification; the ridge count between minutiae A and B is 1, while the ridge count between minutiae B and C is 2.

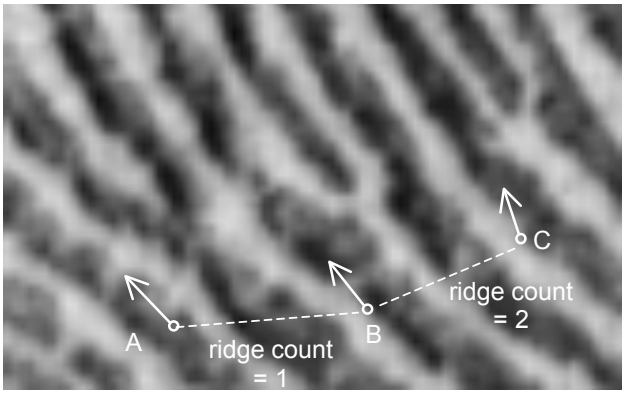


Figure 5 - Example Ridge Count data

7.5.2.1 Ridge Count Extraction Method

The ridge count data area shall begin with a single byte indicating the ridge count extraction method. Ridge counts associated with a particular center minutiae point are frequently extracted in one of two ways: by extracting the ridge count to the nearest neighboring minutiae in each of four angular regions (or quadrants), or by extracting the ridge count to the nearest neighboring minutiae in each of eight angular regions (or octants). The ridge count extraction method field shall indicate the extraction method used, as shown in Table 4.

Table 4 - Ridge Count Extraction Method Codes

RCE method field value	Extraction method	Comments
0x00	Non-specific	No assumption shall be made about the method used to extract ridge counts, nor their order in the record; in particular, the counts may not be between nearest-neighbor minutiae
0x01	Four-neighbor	For each center minutiae used, ridge count data was extracted to the nearest neighboring minutiae in four

	(quadrants)	quadrants, and ridge counts for each center minutiae are listed together
0x02	Eight-neighbor (octants)	For each center minutiae used, ridge count data was extracted to the nearest neighboring minutiae in eight octants, and ridge counts for each center minutiae are listed together

If either of these specific extraction methods are used, the ridge counts shall be listed in the following way:

- all ridge counts for a particular center minutiae point shall be listed together;
- the center minutiae point shall be the first minutiae point references in the three-byte ridge count data;
- if a given quadrant or octant has no neighboring minutiae in it, a ridge count field shall be recorded with both the minutiae index and the ridge count fields set to zero (so that, for each center minutiae, there shall always be four ridge counts recorded for the quadrant method and eight ridge counts recorded for the octant method);
- no assumption shall be made regarding the order of the neighboring minutiae.

Example - (Informative) If the extraction method code is 0x01, and ridge counts were extracted for minutiae numbers 5 and 22, the four ridge counts for minutiae number 22 could be listed first, followed by all four ridge counts for minutiae number 5.

7.5.2.2 Ridge Count Data

The ridge count data shall be represented by a list of three-byte elements. The first and second bytes are an index number, indicating which minutiae points in the corresponding minutiae area are being considered. The third byte is a count of the ridges intersected by a direct line between these two minutiae points.

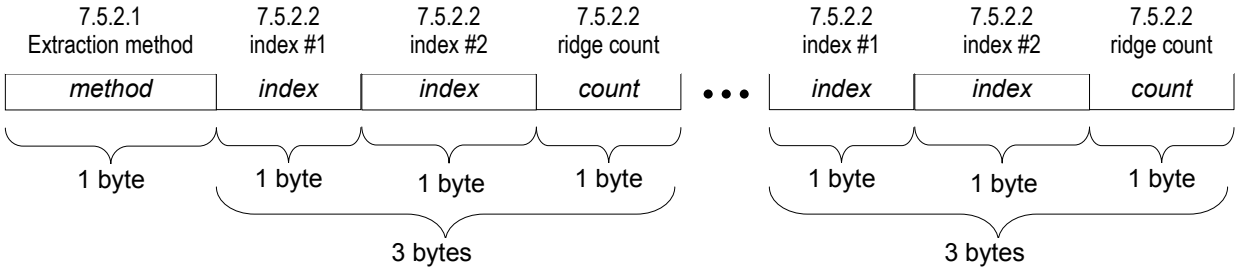
The ridge count data shall be listed in increasing order of the index numbers, as shown in Table 5. There is no requirement that the ridge counts be listed with the lowest index number first. Since the minutiae points are not listed in any specified geometric order, no assumption shall be made about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

Table 5 - Example Ridge Count Data

Minutiae index #1	Minutiae index #2	Ridge count
0x01	0x02	0x05
0x01	0x06	0x09
0x01	0x07	0x02
0x02	0x04	0x13
0x02	0x09	0x0D
0x05	0x03	0x03
0x09	0x15	0x08

7.5.2.3 Ridge Count Format Summary

The ridge count data format shall be as follows:



7.5.3 Core and Delta Data Format

If the extended data area type code is 0x0002, the extended data area contains core and delta information. This format is provided to contain optional information about the placement and characteristics of the cores and deltas on the original fingerprint image. Core and delta points are determined by the overall pattern of ridges in the fingerprint. There may be one or more core points and zero or more delta points for any fingerprint. Core and delta points may or may not include angular information.

The core and delta information shall be represented as follows. The first byte shall contain the core information type and the number of core points included; legal values are 1 or greater. This length byte shall be followed by the position and angular information for the cores. The next byte shall contain the delta information type and the number of delta points included; legal values are 0 or greater. This length byte shall be followed by the position and angular information for the deltas.

7.5.3.1 Core Information Type

The core information type shall be recorded in the first two bits of the upper byte of the number of cores. The bits “00” will indicate that the core has angular information while “01” will indicate that no angular information is relevant for the core type. If this field is “00”, then the angle fields shall not be present for the cores.

7.5.3.2 Number of Cores

The number of core points represented shall be recorded in the least significant four bits of this byte. Valid values are from 0 to 15.

7.5.3.3 Core Position

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

7.5.3.4 Core Angle

The angle of the core shall be recorded in one byte in units of 1.40625 (360/256) degrees. The value shall be a non-negative value between 0 and 255, inclusive. For example, an angle value of 16 represents 22.5 degrees. If the core information type is zero (see Section 6.5.3.1), then this field shall not be present.

7.5.3.5 Delta Information Type

The delta information type shall be recorded in the first two bits of the upper byte of the number of deltas. The bits “00” will indicate that the delta has angular information while “01” will indicate that no angular information is relevant for the delta type. If this field is “00”, then the angle fields shall not be present for the deltas.

7.5.3.6 Number of Deltas

The number of delta points represented shall be recorded in the least significant four bits of this byte. Valid values are from 0 to 15.

7.5.3.7 Delta Position

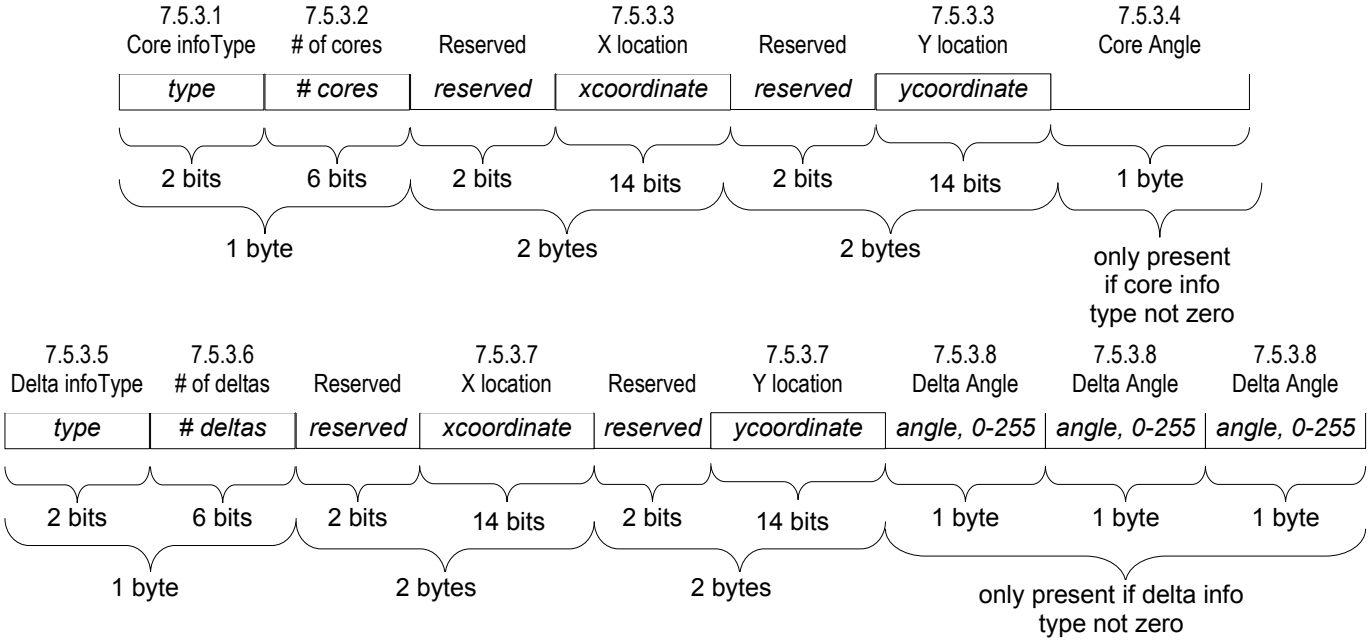
The X coordinate of the delta shall be recorded in the lower fourteen bits of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header.

7.5.3.8 Delta Angles

The three angle attributes of the delta shall be recorded in one byte in units of 1.40625 (360/256) degrees. The value shall be a non-negative value between 0 and 255, inclusive. For example, an angle value of 16 represents 22.5 degrees. If the delta information type is zero (see Section 7.5.3.5), then this field shall not be present.

7.5.3.9 Core and Delta Format Summary

The core and delta format shall be as follows:



7.5.4 Zonal Quality Data

If the extended data area type code is 0x0003, the extended data area contains zonal quality data. This format is provided to contain optional information about the quality of the fingerprint image within each cell in a grid defined on the original fingerprint image. Within each cell, the quality may depend on the presence and clarity of ridges, spatial distortions and other characteristics.

The zonal quality data shall be represented as follows. The first two bytes shall contain the horizontal and vertical cell sizes in pixels. These size bytes shall be followed by the quality indications for each cell, with one bit for each cell. The cell quality bits shall be packed into bytes, padded with zeroes on the right to complete the final byte. All cells are the same size, with the exception of the final cells in each row and in each column. The final cell in each row and in each column may be less than the stated cell size, if the cell width and height are not factors of the image width and height respectively.

7.5.4.1 Cell Width and Height

The number of pixels in cells in the x-direction (horizontal) shall be stored in one byte. Permissible values are 1 to 255.

The number of pixels in cells in the y-direction (vertical) shall be stored in one byte. Permissible values are 1 to 255.

7.5.4.2 Cell Data Length

The number of bytes containing the cell quality data shall be recorded in two bytes. The contents of this field shall be equal to the pixel width in the original image divided by the cell width, rounded up, multiplied by the pixel height of the original image divided by the cell height, rounded up, then divided by eight and rounded up.

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

where the function ceil() indicates the smallest integer greater or equal to the inner quantity. This field is included for convenience in reading the data record.

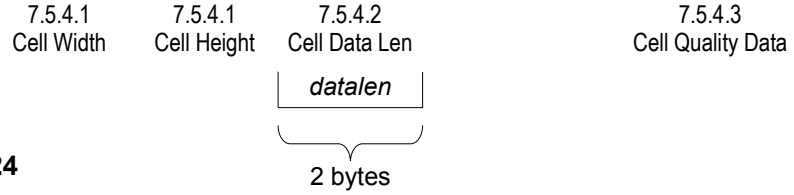
7.5.4.3 Cell Quality Data

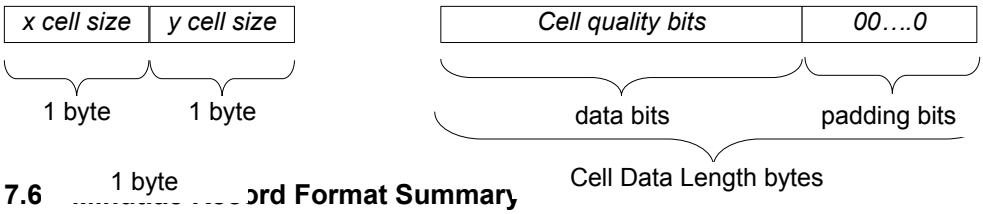
The quality of the fingerprint image in each cell shall be represented by one bit. If the finger image within this cell is of good clarity and significant ridge data is present, the cell quality shall be represented by the bit value '1'. If the cell does not contain significant ridge data, or the ridge pattern within the cell is blurred, broken or otherwise of poor quality, the cell quality shall be represented by the bit value '0'.

The cell quality shall be packed into bytes. The final byte in the cell quality data may be packed with bit values of zero ('0') on the right as required to complete the last byte.

7.5.4.4 Zonal Quality Data Format Summary

The zonal quality data format shall be as follows:





1 byte

7.6 ord Format Summary

Table 6 is a reference for the fields present in the Finger Minutia Record format. Optional extended data formats for ridge counts and core and delta information are not represented here. For more specific information, please refer to the text and to the Record Format Diagrams in Annex A.

Table 6 - Minutiae Record Format Summary

		Field	Size	Valid Values	Notes
One per record		Format Identifier	4 bytes	0x464D5200 ('F' 'M' 'R' 0x0)	"FMR " – finger minutiae record
		Version of this standard	4 bytes	n n n 0x0	" XX"
		Length of total record in bytes	4 bytes	26 – 65535, or 65536 - 4294967295	either 0x001A to 0xFFFF, or 0x000000010000 to 0x0000FFFFFFFF
		Capture Equipment Certification	4 bits		
		Capture Equipment ID	12 bits		Vendor specified
		Image Size in X	2 bytes		in pixels
		Image Size in Y	2 bytes		in pixels
		X (horizontal) Resolution	2 bytes		in pixels per cm
		Y (vertical) Resolution	2 bytes		in pixels per cm
		Number of Finger Views	1 byte	0 to 255	
		Reserved byte	1 byte	00	0 for this version of the standard
One per finger view		Finger Position	1 byte	0 to 11	Refer to ANSI/NIST standard
		View Number	4 bits	0 to 15	
		Impression Type	4 bits	0 to 3 or 8	
		Finger Quality	1 byte	0 to 100	0 to 100
		Number of Minutiae	1 byte		
One per minutia		X (minutia type in upper 2 bits)	2 byte		Expressed in image pixels
		Y (upper 2 bits reserved)	2 byte		Expressed in image pixels
		θ	1 byte	0 to 255	Resolution is 1.40625 degrees
		Quality	1 byte	0 to 100	1 to 100 (0 indicates "quality not reported")
One per view		Extended Data Block Length	2 bytes		0x0000 = no private area
Zero or more per view		Type Code for Extended Area	2 bytes		only present if Extended Data Block Length ≠ 0
		Length of extended data area	2 bytes		only present if Extended Data Block Length ≠ 0
		Extended data area	In prev. field		only present if Extended Data Block Length ≠ 0
		Each extended data area may contain vendor-specific data, or one of the following:			
Zero or more per view	Ridge count data	Ridge count extraction method	1 byte	0 to 2	
		Ridge count data – idx #1	1 byte	1 to # of minutiae	
		Ridge count data – idx #2	1 byte	1 to # of minutiae	
		Ridge count data – count	1 byte		
		additional ridge counts…			
Zero or more per view (may precede ridge count block)	Core and delta data	Core information type	2 bits	0 to 1	
		Number of cores	4 bits	0 to 15	
		X location	2 bytes		
		Y location	2 bytes		
		Angle (*if core info type ≠ 0)*	1 byte	0 to 255	
		Delta information type	2 bits	0 to 1	
		Number of deltas	4 bits	0 to 15	
		X location	2 bytes		
		Y location	2 bytes		
		Angles (*if delta info type ≠ 0)*	3 bytes	0 to 255	
	Zone quality	Cell Width	1 byte	1 to 255	
		Cell Height	1 byte	1 to 255	
		Cell Data Length	2 bytes	1 to 65536	
		Cell Quality Data	CellDataLen		

8 Finger Minutiae Card Format

This standard defines two card related encoding formats for finger minutiae, the normal size format and the compact size format. Such a format may be used e.g. as part of a Biometric Information Template as specified in ISO/IEC 7816-11 with incorporated CBEFF data objects, if off-card matching is applied, or in the command data field of a VERIFY command, if match-on-card (MOC) is applied (see ISO/IEC 7816-4 and -11).

NOTE – The term “card” is used for smartcards as well as for other kind of tokens.

8.1 Normal Size Finger Minutiae Format

With the normal size format, a minutia is encoded in 5 bytes (see Table 12):

- minutia type t (2 bits):
  00 = other,
  01 = ridge ending (encoded as valley skeleton bifurcation point), or ridge skeleton end point
  10 = ridge bifurcation (encoded as ridge skeleton bifurcation point)
  11 = reserved for future use

- coordinate x (14 bits), unit = 10^{-2} mm

- reserved (2 bits), default value: 00

- coordinate y (14 bits), unit = 10^{-2} mm

- angle θ (8 bits), unit = $2\pi/256$

Table 12 — Normal size finger minutiae format

type t	x-coordinate	reserved	y-coordinate	angle θ
2 bytes		2 bytes		1 byte

8.2 Compact Size Finger Minutiae Format

With the compact size format, only 3 bytes are used per minutia (see Table 13). This reduction of memory space is only possible at the cost of a reduction in resolution of coordinates and angle.

- coordinate x (8 bits), unit = 10^{-1} mm
- coordinate y (8 bits), unit = 10^{-1} mm
- minutia type t (2 bits): same coding as with the normal size format

- angle θ (6 bits), unit = $2\pi/64$

Table 13 — Compact size finger minutiae format

x-coordinate	y-coordinate	type t	angle θ
1 byte	1 byte	1 byte	

NOTE - The maximum value for the x and y coordinate is 25.5mm with the compact format.

8.3 Number of Minutiae, Minutiae Ordering Sequence and Truncation

8.3.1 General Aspects

The minutiae data of a finger consist of n minutia encoding shown in Table 12 (or alternatively Table 13). The number n depends on

- the minimum number of minutiae required according to the security level (see Annex C)
- the maximum number of minutiae accepted by a specific card e.g. due to buffer restrictions and computing capabilities.

The maximum number of minutiae accepted is therefore an implementation dependent value and shall be indicated in the Biometric Information Template, if the default value is not used (see Annex C).

A card may also require a special ordering of the minutiae presented in the biometric verification data. The ordering scheme shall be indicated in the Biometric Information Template (see ISO/IEC 19785 and ISO/IEC 7816-11), if the default value is not used.

If the number of minutiae exceeds the maximum number processible by a card, truncation is necessary. The truncation is a 2 step process. At first, finger minutiae of poor quality are eliminated. If still too many minutiae are there, then truncation shall be made by peeling off minutiae from the convex hull of the minutiae set and before sorting into the order required by the card.

8.3.2 Biometric matching algorithm parameters

Biometric matching algorithm parameters are used to indicate implementation specific values to be observed by the outside world when computing and structuring the biometric verification data. They can be encoded as DOs embedded in a biometric matching parameter template as defined in ISO/IEC 19785 (CBEFF Annex D, Table D.1).

8.3.3 Number of Minutiae

For the indication of the minimum and maximum value of minutiae expected by the card the DO Number of minutiae as shown in Table 14 shall be used.

Table 14 – Data Object for Number of Minutiae

Tag	L	Value
´81´	2	min (1 byte, binary coding) || max (1 byte, binary coding)

If this DO is not present in the BIT, the default values apply (see Annex C).

8.3.4 Minutiae Order

For the indication of the ordering scheme for minutiae, the DO Minutiae order as shown in Table 15 shall be used.

Table 15 – Data Object for Minutiae Order

Tag	L	Value
´82´	1	see Table 16

Table 16 – Values for Minutiae Order Indication

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	no ordering required (default value)
						0	1	ordered ascending
						1	0	ordered descending
			0	0	1			Cartesian x-y, see note 1
			0	1	0			Cartesian y-x
			0	1	1			Angle, see note 2
			1	0	0			Polar, root = center of mass
x	x	x						000, other values are RFU

NOTES –

1. Ordered by ascending/descending x-coordinate, if equal by ascending/descending y-coordinate (first x, then y)
2. The angle represents the orientation of the minutia.

The following description defines the ordering procedure in detail to avoid misunderstandings or misinterpretations.

Ordered ascending

Ordered ascending means, that the ordered sequence begins with the minutia from the original minutiae set, that has the smallest value of the indicated item. The value of this item increases with every successive minutia to the maximum value in the last minutia of the ordered sequence.

Ordered descending

Ordered descending means, that the ordered sequence begins with the minutia from the original minutiae set, that has the largest value of the indicated item. The value of this item decreases with every successive minutia to the minimum value in the last minutia of the ordered sequence.

Cartesian x-y

Cartesian x-y stands for an ordering scheme, where first the x-coordinate is compared and used for ordering. When ordering by ascending Cartesian x-y coordinates, the minutia with minimum x-coordinate becomes the first minutia in the ordered sequence. The minutia with the second smallest x-coordinate becomes the second minutia in the ordered sequence. This process continues until the minutia with maximum x-value becomes the last minutia in the ordered sequence. If the x-coordinates in two or more minutiae are equal, the y-coordinate is compared for ordering.

Cartesian y-x

Cartesian y-x stand for an ordering scheme, where first the y-coordinate is compared and used for ordering. If the y-coordinates in two or more minutiae are equal, the y-coordinate is compared for ordering.

Angle

Sorting a minutiae list by angle is done as follows. As defined in a previous section the angle of a minutia begins with value 0 to the right horizontal axis and increases counter-clockwise. When ordering by increasing angle, the minutia with the minimum angle value in the ordered sequence becomes the first minutia in the ordered sequence. The minutia with the second smallest angle value becomes the second minutia in the ordered sequence. This process continues until the last minutia in the ordered sequence is defined as the minutia with maximum angle value. No rules for subordering are defined, if the angle values in two or more minutiae are equal. Any possible ordering sequence of the minutiae with the same angle value is legal in this case.

Polar

Polar is an ordering sequence by ascending or descending polar coordinates. First of all, a virtual coordinate root is defined as the center of mass of all minutiae. The polar coordinates of every minutiae are computed as the relative distance and angle to this root coordinate. Without loss of generality, the process of ascending ordering with polar coordinates is described. The minutia with minimum distance to the root becomes the first minutia in the ordered sequence. The minutia with the second smallest distance to the root becomes the second minutia in the ordered sequence. This process continues until the minutia with maximum distance to the root becomes the last minutia in the ordered sequence. If the root-distance of two minutiae or more is equal, the angle of these minutiae is compared. The minutia with the smallest relative angle value becomes the next minutia in the ordered sequence.

NOTE –
To compute the position of the center of mass of a list of minutiae, the minutiae are considered as objects in a two-dimensional plane acting together as a single entity. The location of the centre of mass can be calculated if the mass m_i and location (x_i, y_i) of each component is known. By definition the centre of mass is located at (x_{com}, y_{com}) where

$$x_{com} = (m_1x_1 + m_2x_2 + ...) / (m_1 + m_2 + ...)$$
$$y_{com} = (m_1y_1 + m_2y_2 + ...) / (m_1 + m_2 + ...)$$

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

$$x_{cm} = (x_1 + x_2 + ... + x_n) / n$$
$$y_{cm} = (y_1 + y_2 + ... + y_n) / n$$

9 CBEFF Format Owner and Format Types

Format owner and format type are encoded according to CBEFF. The format owner is ISO/IEC JTC 1/SC 37. The IBIA registered format owner id is ’0101’.

The format type denotes one of the finger minutiae formats according to this standard, see Table 18.

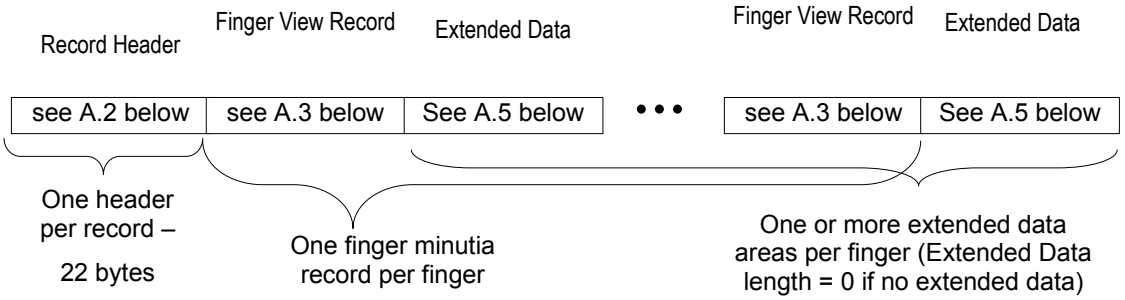
Table 18 — Format types

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

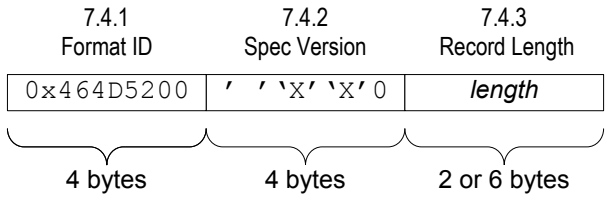
Annex A
(normative)

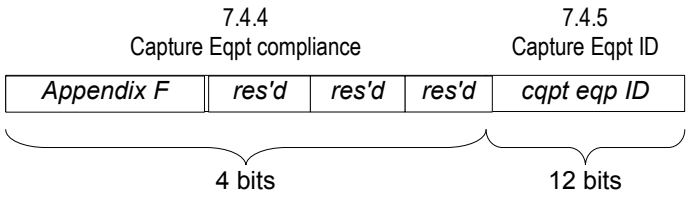
Record Format Diagrams

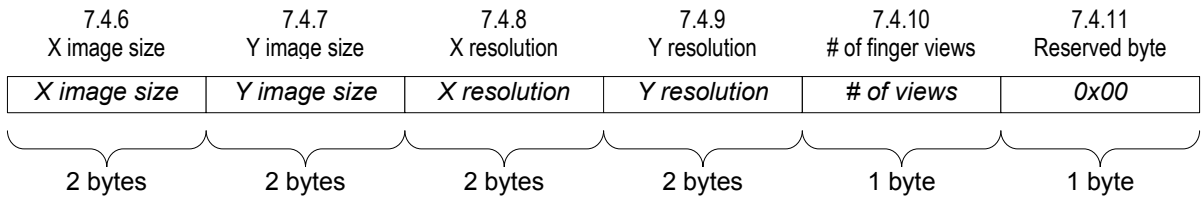
A.1 Overall Record Format



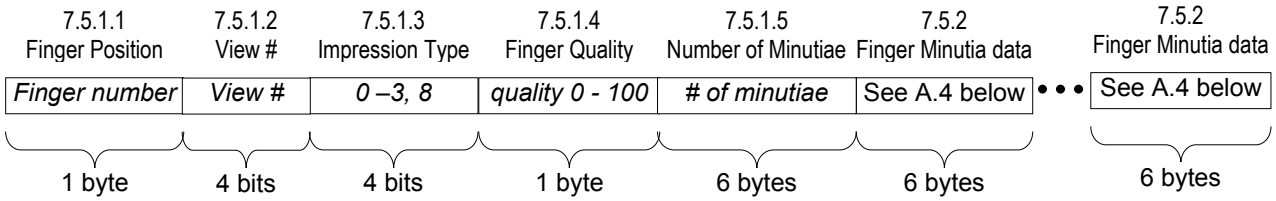
A.2 Record Header



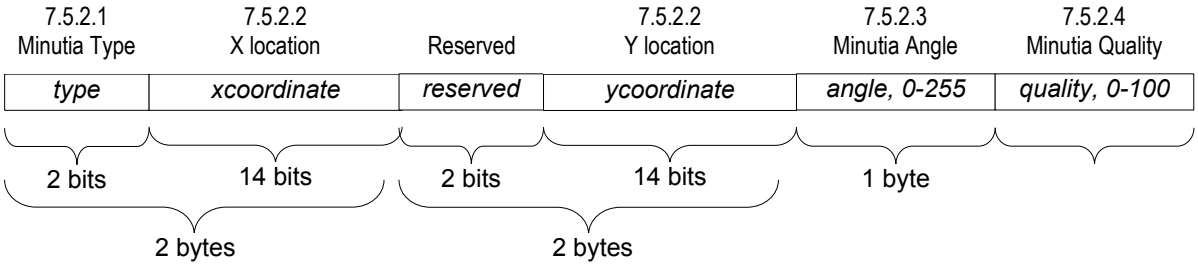




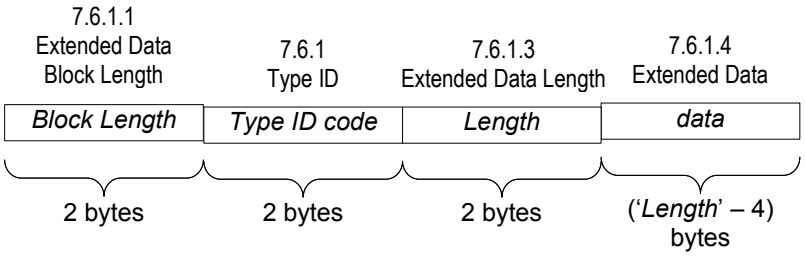
A.3 Single Finger View Minutiae Record



A.4 Finger Minutiae Data



A.5 Extended Data



Annex B
(informative)

Example Data Record

This example minutiae record demonstrates the format for a given set of data.

B.1 Data

Scanner ID = 0x00B5 (these values are determined by the IBIA - for the Vendor ID - and by the vendor)

Sensor Resolution: 500 dpi in both X and Y axes; 196.85 pixels per cm, Image was 512 by 512 pixels

Plain live-scan prints of the left and right index fingers

Left Index: Finger quality is 90% of the maximum possible; 27 minutia, listed in table below; no private feature data

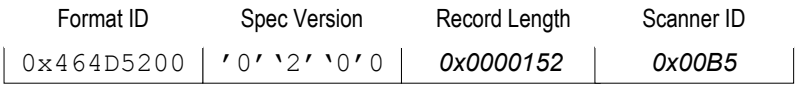
Right Index: Finger quality is 70% of the maximum possible; 22 minutia, listed in table below. Private feature data area (Type 01) consisting of six bytes: 0x01, 0x44, 0xBC, 0x36, 0x21, 0x43

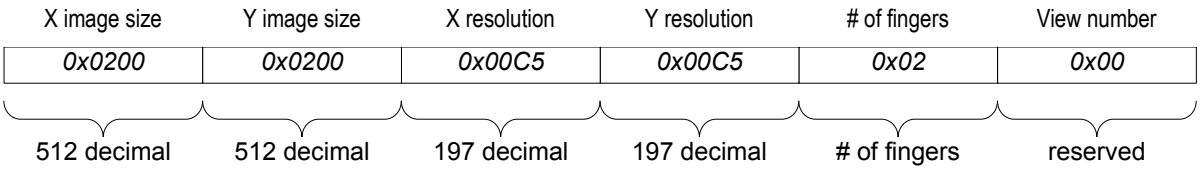
Record length = 340 = 26 (record header) + 2 * 4 (finger headers) + 27 * 6 (minutia for 1st finger) + 22 * 6 (minutia for 2nd finger) + 2 (null private area for 1st finger) + 10 (private area for 2nd finger)

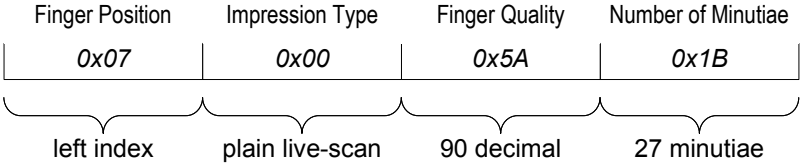
Minutia	Left Index Finger					Right Index Finger				
#	Type	X	Y	Angle	quality	Type	X	Y	Angle	quality
0	Ending	100	14	112	90	ending	40	93	0	90
1	Ending	164	17	85	80	bifurcation	116	100	0	80
2	Bifurcation	55	18	22	90	ending	82	95	12	70
3	Bifurcation	74	22	76	60	bifurcation	140	113	15	70
4	Ending	112	22	90	80	ending	122	135	18	80
5	Bifurcation	42	31	44	90	bifurcation	55	72	21	50
6	Bifurcation	147	35	51	90	ending	94	74	24	60
7	Ending	88	38	165	40	ending	155	62	42	80
8	Bifurcation	43	42	4	80	bifurcation	42	64	55	70
9	Ending	56	48	33	70	ending	155	85	59	80
10	Ending	132	49	72	90	bifurcation	96	192	62	80
11	Bifurcation	71	50	66	80	ending	114	86	85	80
12	Other	95	51	81	90	bifurcation	142	90	90	70
13	Ending	112	53	132	50	ending	57	137	100	90
14	Bifurcation	135	58	32	80	ending	131	75	110	80
15	Other	41	60	59	70	ending	45	113	120	80
16	Bifurcation	67	62	145	90	bifurcation	111	171	130	50
17	Ending	91	63	132	80	ending	95	62	150	60
18	Ending	112	65	33	60	bifurcation	61	114	200	80
19	Ending	53	71	45	90	bifurcation	143	72	250	80
20	Bifurcation	104	74	12	80	ending	63	104	300	70
21	Ending	75	79	21	90	bifurcation	125	73	350	40
22	Bifurcation	48	80	92	90					
23	Ending	130	89	45	80					
24	Bifurcation	63	95	126	80					
25	Ending	47	108	164	90					

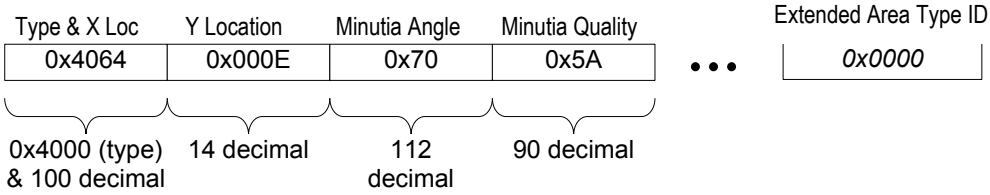
26	Bifurcation	126	115	172	30					

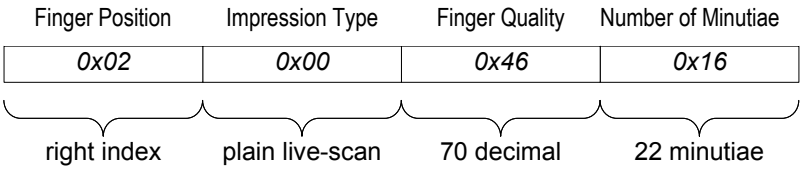
B.2 Example Data Format Diagrams

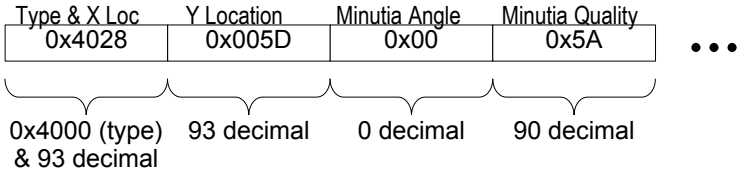


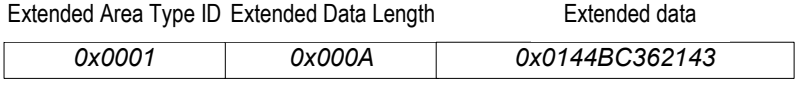












B.3 Raw Data for the Resulting Minutiae Record

Record Header:

0x464D520030323000015200B50200020000C500C50200

1st Finger Header:

0x07005A1B

1st Finger Minutiae data:

0x4064000E505A	0x40A400113C50	0x80370012105A
0x804A0016363C	0x407000164050	0x802A001F1F5A
0x80930023245A	0x405800267528	0x802B002A0350
0x403800301746	0x40840031335A	0x804700322F50
0x005F00333A5A	0x407000355E32	0x8087003A1750
0x0029003C2A46	0x8043003E675A	0x405B003F5E50
0x40700041173C	0x40350047205A	0x8068004A0950
0x404B004F0F5A	0x80300050415A	0x408200592050
0x803F005F5A50	0x402F006C755A	0x807E00737A1E

1st Private Data Area:

0x0000

2nd Finger Header:

0x02004616

2nd Finger Minutiae data:

0x4028005D005A	0x807400640050	0x4052005F0946
0x808C00710B46	0x407A00870D50	0x803700480F32
0x405E004A113C	0x409B003E1E50	0x802A00402746
0x409B00552A50	0x806000C02C50	0x407200563C50
0x808E005A4046	0x40390089475A	0x4083004B4E50
0x402D00715550	0x806F00AB5C32	0x405F003E6B3C
0x803D00728E50	0x808F0048B250	0x403F0068D546
0x807D0049F928		

2nd Private Data Area:

0x0001000A0144BC362143

Annex C
(informative)

Handling of Finger Minutiae Card Formats

C.1 Enrollment

C.1.1 Number of minutiae

The number of minutiae is a security sensitive parameter and depending on the security policy of the application. Persons who do not meet the minimum required number for enrolment cannot be enrolled. The maximum number of minutiae for the reference data is implementation dependent.

The recommended minimum number of minutiae required for enrollment is 16 and for verification is 12. The strength of function (see note at the end of this clause) may have impact on these values.

The maximum number of minutiae to be sent to a card is implementation dependent and related to:

- transmission time
- memory resources
- execution time
- security aspects

The recommended maximum value for enrollment and verification is 60. It is up to the extraction device to limit the number of minutiae sent to the card to 60 or the indicated value (see CBEFF Annex G, Table G.1).

NOTE - In the Common Criteria, the following definitions are given:

Strength of Function (SOF) — A qualification of a Target of Evaluation (TOE) security function expressing the minimum efforts assumed to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic — A level of TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium — A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high — A level of TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

C.1.2 Number of required finger presentations

The number of required finger presentations during an enrollment process is enrollment system dependent.

C.2 Matching

The verification data is subject to translation (in x- and y-direction), rotation (deviation of the orientation) and distortion. Matching also has to take into account components or factors like FAR/FRR.

C.2.1 Matching conditions

The result of the matching process is a score, which may denote the number of matching minutiae or any other appropriate value. In interoperability tests, it may be verified whether different implementations of the matching algorithm meet a required FAR/FRR e.g. in relation to the strength of function for the respective application.

If minutia types are taken into account in the matching process, the different types match according to Table .

Table C.1 - Minutiae type matching

Type of verification minutiae	Match with type of reference minutiae
00	00, 01, 02
01	00, 01
02	00, 02
00 = other 01 = ridge ending (encoded as valley skeleton bifurcation point), or ridge skeleton end point, see note 02 = ridge bifurcation (encoded as ridge skeleton bifurcation point)	

NOTE – The alternatives depend on the format type.

C.2.2 Threshold Value

A verification decision result is positive (i.e. the user verification is successful), if the score S as matching result is greater or equal than the required threshold value T:

$S \geq T$

The threshold value depends on several factors or components such as

- Required False Acceptance Rate FAR
- Required False Rejection Rate FRR
- Matching conditions, see 7.2.1
- The amount of minutiae enrolled
- The amount of minutiae presented
- Strength of function.

The treatment of the threshold value is dependent on the implemented matching strategy. In the following an example of the calculation of a threshold value is presented.

The threshold value T considered in this example is a dynamic value to be calculated for each verification process and depends on:

- Ar: amount of minutiae in the reference data
- Av: amount of minutiae in the verification data
- Avmin: minimum amount of minutiae required in the verification data
- Avmax: maximum amount of minutiae in the verification data relevant for threshold computation
- Tmin: minimum threshold value, which denotes the minimum amount of minutiae to be matched for positive verification
- Tmax: maximum threshold value, which denotes the maximum required amount of minutiae to be matched for positive verification.

T is computed as follows:

$T = Tmin + (Ac – Avmin) * (Tmax – Tmin)/(Avmax – Avmin)$

with

$Ac = qAr + (1 – q)Av,$

whereby Ac is the calculated amount of minutiae and the qualifier q the weight for Ar and Av

and

Avmin = min. amount of minutiae to be presented in a verification process

Avmax = max. amount of minutiae considered relevant in a verification process.

The values of Tmax, Tmin, Avmax, Avmin and q chosen for this example are shown in .

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

Qualifier q	Tmin	Tmax	Avmin	Avmax
0.66	6	12	12	60

The values in Table A.1 together with the above formula have the following meaning:

- the amount of the reference minutiae have more significance than the amount of the verification minutiae (2/3 to 1/3)
- a score of 4 matching minutiae is generally rejected and leads to a negative verification result (S < T, Tmin required = 6)
- a score of 5 matching minutiae leads to positive verification (S ≥ T), if the respective person has a minimum of verification minutiae (12)

- a score of 12 matching minutiae leads in any case to a positive verification (Tmax required = 12).

NOTE: At court, some countries require 12 matching minutiae. However, the application area, the environment conditions and security requirements are different at court and for on-card-matching.

C.2.3 Retry Counter

For on-card matching, a retry counter (which is decremented by subsequent negative verifications and set to its initial value by positive verification) has to be implemented in order to limit the number of trials. The following aspects have impact on the initial value:

- experience of the user
- environmental conditions (e.g. construction of sensor embedding and finger placement)
- quality of verification data
- strength of function.

If the retry counter has reached the value 0, then the respective biometric verification method is blocked. Resetting the retry counter to its initial value is possible, if supported, e.g. by using the RESET RETRY COUNTER command (see ISO/IEC 7816-4) with a resetting code (8 digits).

The recommended initial value of the retry counter lies in the range of 5 and 15. The security policy of the application provider and the required strength of function have impact on the possible range and the value applied.

C.3 Security Aspects of Finger Minutiae Presentation to the Card

Fingerprints are left everywhere and therefore this kind of biometric data are considered to be public. An attacker may succeed in getting a good fingerprint of a person, derive from them the biometric verification data and present it to the stolen card of the respective person. To avoid this kind of attack and also replay attacks of data used in a previous verification process, a trusted path between card and service system is required. Such a trusted path is achieved by cryptographic means, e.g. using secure messaging according to ISO/IEC 7816-4. The specification of those secure messaging functions is usually application dependent and outside the scope of this standard.

Bibliography

[1] ANSI/NIST ITL 1-2000 „Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information" (NIST Special Publication 500-245)

[2] A. Jain, S. Pankanti: "Fingerprint Classification and Matching", Michigan State University, 1999 <need a better citation>

[3] S. Pankanti, S. Prabhakar, A. Jain: „On the Individuality of Fingerprints", in IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002

[4] AAMVA Driver License Standard 20000630 — Annex C: Finger Imaging, 2000

[5] ISO/IEC FDIS 7816-4:2003, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange.*

[6] ISO/IEC FDIS 7816-6:2003, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange.*

[7] ISO/IEC FDIS 7816-11:2003, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods.*

[8] ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER); Technical Corrigendum 2*

Annex D

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

Please see Annex D, in Appendix I.