INTERNATIONAL LABOUR ORGANIZATION

Seafarers’ Identity Documents Convention (Revised), 2003 (No. 185)

The standard for the biometric template required by the Convention

Geneva, 2006

INTERNATIONAL LABOUR OFFICE GENEVA

INTERNATIONAL LABOUR ORGANIZATION

Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)

The standard for the biometric template required by the Convention*

Geneva, 2006

* This standard was adopted by the Governing Body at its 289th Session (March 2004) and amended at its 294th Session (November 2005).

INTERNATIONAL LABOUR OFFICE GENEVA

ISBN: 92-2-118217-7 (print)
92-2-118218-5 (web print)

First published 2004

Second impression (with modifications) 2006

The designations employed in ILO publications, which are in conformity with United Nations practice, and the presentation of material therein do not imply the expression of any opinion whatsoever on the part of the International Labour Office concerning the legal status of any country, area or territory or of its authorities, or concerning the delimitation of its frontiers.

The responsibility for opinions expressed in signed articles, studies and other contributions rests solely with their authors, and publication does not constitute an endorsement by the International Labour Office of the opinions expressed in them.

Reference to names of firms and commercial products and processes does not imply their endorsement by the International Labour Office, and any failure to mention a particular firm, commercial product or process is not a sign of disapproval.

ILO publications can be obtained through major booksellers or ILO local offices in many countries, or direct from ILO Publications, International Labour Office, CH-1211 Geneva 22, Switzerland. Catalogues or lists of new publications are available free of charge from the above address, or by email: pubvente@ilo.org

Visit our web site: www.ilo.org/publns

Printed by the International Labour Office, Geneva, Switzerland

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.

The ISO and the International Electrotechnical Commission (IEC) form the specialized system for worldwide standardization. National bodies that are members of the 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 the 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, the 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). The 2004 version of this report was submitted as a technical contribution to ISO/IEC JTC 1 Subcommittee (SC) 37, *Biometrics*.

This report, ILO SID-0002 revision, *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 – 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 requirements;
- section 5.3 – SID identity verification requirements;
- section 5.4 – SID database requirements.

Contents

Page

Annexes

Acknowledgements

The editors of this report for the International Labour Office (ILO) were Ms. Cynthia L. Musselman, Dr. Valorie S. Valencia and Mr. Michael R. Crusoe of Authenti-Corp and Dr. John W. M. Campbell of Bion Biometrics. The ILO also benefited from the comments and contributions of a number of other biometric experts. The International Organization for Standardization (ISO) has kindly permitted the ILO to incorporate the Committee draft standard, which is appended to this report. The ILO extends its sincere appreciation to the ISO.

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 and 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' ID Convention in 2003, which outlined high-level requirements for biometric-based personal identification of the international seafarer community and mandates global interoperability of SID biometric data. The authors submit this technical report, ILO SID-0002 revision, 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 (Convention No. 185, Annex I and Annex II, respectively).

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 International Labour Organization 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 Final Committee Draft (FCD) 19784 – Information technology – Biometric application programme interface (BioAPI) (ISO/IEC JTC 1/SC 37 N 55, 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.[1]

- ISO/IEC Committee Draft (CD) 19785 – Information technology – Common biometric exchange formats framework (CBEFF) (ISO/IEC JTC 1/SC 37 N 208, dated 14 July 2003).

- ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003).

- The International Civil Aviation Organization (ICAO) standard (document 9303) for machine-readable travel documents (MRTDs), commissioned by ISO/IEC JTC 1 SC 17.

  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' ID 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 15415:2004 (PDF417 bar code print quality) are fundamentally applicable to this biometric profile.

Together the standards ISO/IEC 15438:2001, ISO/IEC 15415:2004, ISO/IEC CD 19794-2, ISO/IEC FCD 19784 (ANSI/INCITS 358:2002), and ICAO 9303, represent the foundation upon which the biometric capabilities of the seafarers' ID systems will be built. Other standards 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.

[1] SC 37 N 55, dated 17 December 2002, contains an exact reproduction of ANSI/INCITS 358:2002 – Information technology – BioAPI Specification. While SC 37 draft standards are not openly available to the public, ANSI/INCITS 358:2002 can be obtained at http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=10.

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. This report, ILO SID-0002, represents the technical requirements for the finger *minutiae*-based biometric option, which has been selected as the best-fit solution for the ILO SID application requirements.

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 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/SC 37 N, 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 SID programme.

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

(6) Marine environmental issues, including saline crystalline corrosion issues, are out of the 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 BioAPI_BIR data 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 two related SC37 draft standards: FCD 19784 and CD 19794-2 (referenced in section 3.1). As noted in section 1, a copy of CD 19794-2 is presented in Annex C. FCD 19784 is available as indicated in section 3.1. This biometric profile, and the dated draft standards referenced herein, take precedence for the seafarers' ID should evolution of the draft standards create any perceived inconsistency.

3.1. Normative standards

(a) ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (ISO/IEC JTC 1/SC 37 N 55, dated 17 December 2002). Also available as ANSI/INCITS 358:2002 – Information technology – BioAPI specification. [2]

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

(c) ISO/IEC 15415:2004 – 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 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003).

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

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

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

3.2. Informative references

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

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

(k) 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

(l) SID application profile standard.

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

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

[2] SC 37 N 55, dated 17 December 2002, contains an exact reproduction of ANSI/INCITS 358:2002 – Information technology – BioAPI Specification. While SC 37 draft standards are not openly available to the public, ANSI/INCITS 358:2002 can be obtained at http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=10.

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. Big-endian

A method of data storage in which the least significant byte of a value spanning multiple bytes is in the highest addressed byte.

4.1.3. Biometric

Pertaining to biometrics

Note: "biometric" should not be used as a noun.

4.1.4. Biometric authentication

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

4.1.5. Biometric data block (BDB)

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

4.1.6. Biometric identification

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

4.1.7. 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.

4.1.8. 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. Biometric enrolment

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

4.1.11 Biometrics

The automated recognition of individuals based on their behavioural and biological characteristics.

4.1.12. Country code

The numeric three-digit country code defined in ISO 3166-1:1997.

4.1.13. 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.

4.1.14. 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.

4.1.15. Endian

The method a computer uses to store a multi-byte piece of data.

4.1.16. 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.

4.1.17. Little-endian

A method of data storage in which the most significant byte of a value spanning multiple bytes is in the highest addressed byte.

4.1.18. Null-padded

Filled to the end of a fixed length with zero bytes (0x00).

4.1.19. 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.

4.1.20. Seconds since the epoch (SSE)

Seconds since the epoch (1 January 1970) 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.

4.1.21. Shall

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

4.1.22. Should

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

4.1.23. 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 along 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;” (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;" (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;" (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;" (Convention No. 185, Article 3, paragraph 8(d)).

  This presumes that the biometric and card reading systems will be able to be reliably used onboard 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." (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. [3] If the index fingerprint is missing or damaged to the extent that a reliable fingerprint either

[3] 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).

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 or her reference biometric data, which will be stored on his or 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 of a primary and secondary finger 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 templates corresponds to the fingerprints enrolled and are operationally acceptable to the seafarer; providing a match indication (identity verified) if the matching score is above the matching threshold to be used for verification (see 5.3.1 Biometric verification procedure 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.

If a seafarer is only able to enrol a single finger, even after all available fingers have been tried, then the enrolled finger shall be designated as the primary finger and the secondary finger in the two finger template described in Annex B of this report shall be assigned the characteristics of an "unenrolled finger". If no fingers can be enrolled, then both the primary and secondary fingers in the two finger template shall be assigned the characteristics of an "unenrolled finger".

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 the minimum fingerprint data capture quality level specified below:

- scan resolution: 197 pixels/cm (500 pixels/inch);

- pixel scale depth: 8 bits;

- dynamic range (grey levels): 220.

The fingerprint capture device shall produce an 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

As specified in Annexes B and C, the algorithm shall extract a fingerprint template (biometric information record or BIR) from the acquired fingerprint images in conformance with ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003) and ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (ISO/IEC

JTC 1/SC 37 N 55, dated 17 December 2002 (BioAPI 1.1)[4]). A maximum of 52 minutiae shall be included in each fingerprint template. It is important to note that if the number of minutiae exceeds 52, the truncation process described in Annex B, note 13, shall be followed. The fingerprint templates (BIRs) 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 *minutiae*-based template has been 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. These government databases are typically Automated Fingerprint Information Systems (AFIS) 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 on 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.

- 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 on the document and *it shall not be possible to reconstitute it [understood as "fingerprint image"] from the template or other representation*".

  *Testing of minutiae-based biometric products can be performed to demonstrate that it is **significantly difficult** to reconstitute an exact fingerprint image or to develop a fraudulent device that could be used to misrepresent seafarer intent or presence using data stored in minutiae-based finger templates.* [5]

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

[4] SC 37 N 55, dated 17 December 2002, contains an exact reproduction of ANSI/INCITS 358:2002 – Information technology – BioAPI Specification. While SC 37 draft standards are not openly available to the public, ANSI/INCITS 358:2002 can be obtained at http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=10.

[5] 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.

text 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. This wide range of affordable, commercial bar code reader technology products will facilitate biometric verification by 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 passport (MRP) data page.

- for SID cards the maximum bar code size is 27.8 mm x 85.6 mm [6] including quiet zones (see in 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 (3 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);

[6] 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).

- number of data symbol columns = 16; [7]
- number of rows to contain the data (40 rows). [8]

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 15415:2004 – 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). Note that the SID is an identity document under the terms of ICAO document 9303 in either card or book format. It shall satisfy all print quality and layout requirements specified in the appropriate parts of Document 9303. This includes having a two line (book format) or three line (card format) Machine Readable Zone beginning with the two characters “IS”. The “I” is mandatory and designates the SID as an ID document under the terms of 9303 and the “S” is highly recommended as the secondary identifier, in this case designating it as a Seafarers’ Identity Document.

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 cannot be used.

[7] Mr. Sprague Ackley, an internationally recognized expert in PDF417 2-D bar code technology has indicated that most 2-D imagers should be able to read a bar code containing 16 data columns with an x-dimension of 0.170 mm. He notes, however, that correct printing is very important. The print quality should be checked carefully, since if the print head temperature or lamination temperature are too high then ink spread can degrade the bar code readability. He also recommends that the barcode generation software be configured specifically for the printer being used. In this case, if the printer is 300 dpi, the x-dimension should be set to exactly 2 pixels, if it is 600 dpi, the x-dimension should be set to exactly 4 pixels, etc. Note that if the print technology does not support an even number of pixels in approximately 0.17 mm, this may reduce bar code readability. It is imperative that the process (printing and laminating) for making cards is capable of achieving the print quality grade as stipulated below in 5.2.2. All cards in their final configuration must pass 3.0/05/660 in order to support the application reading environment.

[8] 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 code words. Another 64 code words are required for error correction codes at level 5 plus 1 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. Note that as stated in Annex A, the bar code should be padded to always have 16 data columns by 40 rows.

5.2.4. Bar code physical characteristics

The “biometric template based on a fingerprint printed as numbers in a bar code” (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. (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” (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 finger corresponding to the primary fingerprint template stored in the bar code. If the seafarer’s finger corresponding to the primary finger 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 finger corresponding to the secondary fingerprint template stored in barcode. If either the primary or secondary finger matches the corresponding template stored in the bar code, the seafarer shall be successfully verified. If neither the primary nor secondary fingers match 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 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 at least one 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 Accept Rate (FAR) among the general public of less than 1 per cent and a False Reject Rate (FRR) 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." (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] (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. Seafarers shall be able to verify that the fingerprint templates stored on their card match their enrolled fingers. 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 shall 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 along 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." (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." (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 [Convention No. 185] Annex II are [shall be] entered in the database simultaneously with issuance of the SID". (Convention No. 185, Annex III, Part A, paragraph 3(b)(i).)

  A Member's national electronic database 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." (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". (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." (Convention No. 185, Annex III, Part B, paragraph 4.2.2.)

  A Member's national electronic database 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." (Convention No. 185, Annex III, Part A, paragraph 3(c).)

  A Member's national electronic database 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." (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." (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." (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." (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. (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." (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." (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. (Convention No. 185, Annex III, Part B, paragraph 5.6.5.)

  A Member's national electronic database 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 as described below. The data area shall be padded with enough pad code words (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 personalization data that is both printed on the surface of the SID in text and in the bar code to support seafarer authentication. The bar code fields are described below and shall conform to the formats defined in table A-1. All fields are big-endian except the fingerprint data, which has both big-endian and little-endian fields as described in table B-1 in Annex B.

1. Fingerprint data – data for two-fingerprint templates in BioAPI compliant format.
2. Issuing authority – country code of the issuing authority.
3. Document number – text stream of up to nine characters.
4. Personal identification number – optional text stream of up to 14 characters. A stream of 14 null bytes may be used instead of text.
5. Expiration date – SID date of expiry in seconds since epoch (SSE) format.
6. Primary identification – text stream of up to 20 characters representing the seafarer's primary identifying name.
7. Secondary identification – text stream of up to 20 characters representing the seafarer's secondary identifying name.
8. Nationality – country code representing the seafarer's nationality.
9. Place of birth – text stream of up to 20 characters representing the seafarer's place of birth.
10. Date of birth – seafarer's date of birth in SSE format.
11. Gender – gender of the seafarer, with "male" denoted by character "m," "female" denoted by character "f," and "not specified" denoted by character "x".
12. Date of issue – SID date of issue in SSE format.
13. Place of issue – text stream of up to 20 characters representing the SID place of issue.

Table A-1. SID minutiae-based fingerprint bar code format (normative)

#	Field	Size	Format
1	Fingerprint data	Up to 566 bytes	Specified in Annex B
2	Issuing authority[1]	2 bytes	Unsigned integer representing country code
3	Document number[1]	9 bytes	Text, up to 9 characters[2]
4	Personal identification number	14 bytes	Text, up to 14 characters[2]
5	Expiry date	4 bytes	SSE, unsigned 32-bit integer[3]
6	Primary identifier	20 bytes	Text, up to 20 characters[2]
7	Secondary identifier	20 bytes	Text, up to 20 characters[2]
8	Nationality	2 bytes	Unsigned integer representing country code
9	Place of birth	20 bytes	Text, up to 20 characters[2]
10	Date of birth	4 bytes	SSE, signed 32-bit integer[3]
11	Gender	1 byte	“m” (0x6D), “f” (0x66) or “x” (0x78)
12	Date of issue	4 bytes	SSE, unsigned 32-bit integer[3]
13	Place of issue	20 bytes	Text, up to 20 characters[2]
	Total size	686 bytes	

[1] The name of the issuing authority plus the document number comprises the unique document identifier.

[2] The text fields, fields 3, 4, 6, 7, 9, and 13, shall be null padded to the full size of the field if the data does not fill the field.

[3] Seconds since epoch (SSE) represents the number of seconds since the epoch, 1 January 1970. In SSE format, an unsigned 32-bit integer can represent dates between 1970 and 2106, and a signed 32-bit integer can represent dates between 1901 and 2038. As such, a signed 32-bit integer is used to represent Date of birth (Field 10) and an unsigned integer is used to represent Expiry date (Field 5) and Date of issue (Field 12).

Annex B

SID bar code minutiae-based fingerprint BioAPI_BIR data 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/SC 37 N, dated 7 October 2003)) and the draft ISO/IEC BioAPI specification (ISO/IEC FCD 19784 (ISO/IEC JTC 1/SC 37 N 55, dated 17 December 2002)) to encode two fingerprints with up to 52 minutiae each as specified in the table B-1 below.

The fingerprint BioAPI_BIR data storage format described below constitutes the first field of the SID PDF417 barcode specified in table A-1. This "fingerprint data" field utilizes up to 566 bytes. The remaining fields of the barcode (utilizing 120 bytes) store a digital representation of the text that is printed on the SID (see table A-1).

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 these draft standards create any perceived inconsistency*. A copy of the draft standard ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003) is provided in Annex C, and ISO/IEC FCD 19784 BioAPI (ISO/IEC JTC 1/SC 37 N 55, dated 17 December 2002) is publicly available as ANSI/INCITS 358:2002. [1] 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.

The organization of the BIR format is defined as follows and fully specified in table B-1.

1. A fixed-length (16-byte) BioAPI_BIR_Header containing information about the overall record.
2. The variable-length BioAPI "Opaque biometric data", which includes:

   A fixed-length (22-byte) record header.

   A single finger record for the primary finger consisting of:

   - a fixed-length (4-byte) header containing information about the primary finger data.
   - a series of fixed-length (5-byte) minutia point descriptions, including the position, type, and angle of each primary finger minutia point for up to 52 minutiae.

   A single finger record for the secondary finger consisting of:

   - a fixed-length (4-byte) header containing information about the secondary finger data.
   - a series of fixed-length (5-byte) minutia point descriptions, including the position, type, and angle of each secondary finger minutia point for up to 52 minutiae.

It is important to note that the BioAPI_BIR header is encoded using little-endian format (as defined in ISO/IEC FCD 19784 (ISO/IEC JTC 1/SC 37 N 55, dated 17 December 2002)) whereas the Opaque biometric data is encoded using big-endian format (as defined in ISO/IEC CD 19794-2 (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003)). All values are stored without field delineators. Indexing is by byte-count. Hexadecimal notation is used unless otherwise noted. In no event shall an optional field be skipped. All fields marked as "Fixed" shall contain only the indicated values. Refer

[1] SC 37 N 55, dated 17 December 2002, contains an exact reproduction of ANSI/INCITS 358:2002 – Information technology – BioAPI Specification. While SC 37 draft standards are not openly available to the public, ANSI/INCITS 358:2002 can be obtained at http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=10.

to Annex C for encoding details. Additional guidance and clarification is provided following table B-1.

Table B-1. SID minutiae-based fingerprint BioAPI_BIR storage format (normative)

Field	Size	Value	Comment
BioAPI_BIR_HEADER (16 bytes, little endian) (0x00000sss010401010203nn0100000008)			
Length in bytes	4 bytes	0x00000sss	sss is the size in bytes up to 236, 236 (hex) = 566 (decimal), length of BIR = header (16 bytes) + length of record below (up to 550 bytes) = up to 566 bytes
BioAPI_BIR_VERSION	1 byte	0x01	Fixed
BioAPI_BIR_DATA_TYPE	1 byte	0x04	Fixed – "Processed" data type
BioAPI_BIR_BIOMETRIC_DATA_FORMAT	4 bytes	0x01010203	Fixed – 0x0101 = JTC 1 SC 37 format owner 0x0203 = Finger minutiae card format – normal size
BioAPI_Quality	1 byte	nn	nn is a signed integer with a value of 0 through 100 corresponding to the overall quality of the two stored fingerprints, 0 represents lowest quality, 100 represents highest quality
BioAPI_BIR_PURPOSE	1 byte	0x01	Fixed –"BioAPI_PURPOSE_VERIFY"
Bio_API_BIR_AUTH_FACTORS	4 bytes	0x00000008	Fixed – "BioAPI_FACTOR_FINGERPRINT"
BioAPI_BIR "Opaque biometric data" (up to 550 bytes, big endian)			
Record header (22 bytes)			
Format identifier	4 bytes	0x464D5200	Fixed – "FMR" 0x00, finger minutiae record
Version number	4 bytes	0x20313100	Fixed – ASCII space "11" 0x00, corresponding to version 1.1 [1]
Length of record	2 bytes	Up to 0x0226	Up to 550 bytes, total number of minutiae (up to 104, 52 for each finger) * 5 bytes + 22 bytes record header + 4 bytes primary finger record + 4 bytes secondary finger record)
Capture equipment certification	4 bits		Reserved for implementers' use
Capture equipment ID	12 bits		Reserved for implementers' use
X (horizontal) image size	2 bytes		Pixels
Y (vertical) image size	2 bytes		Pixels
X (horizontal) resolution	2 bytes		Fixed – 1000 or 0x3E8[2]
Y (vertical) resolution	2 bytes		Fixed – 1000 or 0x3E8[2]
Number of fingers[3]	1 byte	0x01	Fixed – Two fingers
Number of finger views[3]	1 byte	0x00	Fixed – One view

Field	Size	Value	Comment
Primary fingerprint record (4 header bytes + up to 260 minutiae bytes)			
Finger number	1 byte	0x01 to 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)
View number	4 bits	0x0	Fixed – One view
Impression type	4 bits	0x0 or 0x8	0x00 = Live-scan plain 0x08 = Swipe
Finger quality	1 byte	0x00 to 0x64	0 to 100, 0 represents lowest quality, 100 represents highest quality
Number of minutiae[4]	1 byte[5]	Up to 0x34	Up to 52 minutiae
Finger minutiae data[6]	Up to 260 bytes		5 bytes per minutiae as indicated below
For each minutiae point:			
Minutiae type[7]	2 bits	0x00, 0x01, 0x02	0x00 = other 0x01 = ridge ending 0x02 = ridge bifurcation
X coordinate	14 bits		1 bit = 10^{-2} mm
reserved	2 bits	0x00	Fixed
Y coordinate	14 bits		1 bit = 10^{-2} mm
Angle[8]	1 byte	0x00 to 0xFF	0 to 255, 1 bit = $2\pi/256$
Total size per minutiae	5 bytes		
Secondary fingerprint record (4 header bytes + up to 260 minutiae bytes)			
Same format as primary fingerprint record			

The “unenrolled” finger (normative)

When a seafarer is only able to enrol a single finger, then that finger is recorded as the primary finger and the secondary finger is recorded as an “unenrolled” finger. If the seafarer can’t enrol any finger, then both primary and secondary fingers are recorded as “unenrolled” fingers. The characteristics of the record for an “unenrolled” finger are as follows:

Table B-2. Characteristics of an “unenrolled” finger

Field	Size	Value	Comment
Unenrolled finger record (4 bytes only)			
Finger number	1 byte	0x00	Fixed
View number	4 bits	0x0	Fixed – One view
Impression type	4 bits	0x0 or 0x8	0x00 = Live-scan plain 0x08 = Swipe
Finger quality	1 byte	0x65 or 0x66	0x65 means enrolment failed due to a

Field	Size	Value	Comment
			physical disability of seafarer 0x66 means enrolment failed due to poor quality fingerprints
Number of minutiae	1 byte	0x00	Fixed

Additional guidance and clarification

[1] The version number “1.1” indicates that there may be differences between ISO/IEC CD 19794-2 (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003) and the final international standard.

[2] From ISO/IEC CD 19794-2 (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003, paragraph 6.3.1) in Annex C. Card normal format has fixed resolution of 1000 pixels per cm.

[3] Note that there is a discrepancy in ISO/IEC CD 19794-2 (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003) in Annex C with respect to the last two fields in the Record header. In paragraphs 7.3.10 and 7.3.11, the last two fields are denoted “Number of fingers” and “View number,” respectively. However, in paragraph A.2, the last two fields are denoted “# of finger views” and “reserved byte”. The prior definition has been employed here.

[4] A maximum of 52 minutiae shall be included in each fingerprint template. If the number of minutiae exceeds 52 after all normal minutiae extraction steps (such as eliminating low quality minutiae), truncation is necessary. Truncation shall remove minutiae in order of largest distance from the centroid of the current minutiae set. If multiple minutiae have the same distance from the centroid and not all of them need too be truncated to reach the 52 minutiae maximum, then minutiae in the same distance group shall be truncated as follows: 1) truncate same distance minutiae with the lowest x-coordinate; 2) if two or more minutiae have the same x-coordinate then truncate starting with the lowest y-coordinate. This truncation procedure takes precedence over that defined in ISO/IEC CD 19794-2, dated 7 October 2003 (ISO/IEC JTC 1/SC 37 N, paragraph 8.3.1) in Annex C.

[5] Note that there is an error in ISO/IEC CD 19794-2 (ISO/IEC JTC 1/SC 37 N, dated 7 October 2003, paragraph A.3) in Annex C. The number of bytes for “Number of minutiae” should be 1, not 6.

[6] To enable interoperability, the matching algorithm shall not require a particular order of the minutiae in the fingerprint record.

[7] To enable interoperability, the matching algorithm shall be capable of matching even if some or all minutiae are of the “other” type. In other words, the matching algorithm shall function accurately without knowledge of minutiae type in the enrolment template.

[8] Minutiae angles shall be encoded using the using the full resolution of angle measurement specified in ISO/IEC CD 19794-2, dated 7 October 2003 (ISO/IEC JTC 1/SC 37 N, paragraph 8.1) in Annex C. Specifically, the angle should be calculated and encoded to the nearest $2\pi/256$ unit. If larger quantization units are used to calculate the angle, such as $2\pi/16$, interoperability performance may be degraded.

Annex C

ISO/IEC JTC 1/SC 37 N

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
STD Version 2.1

Contents

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.

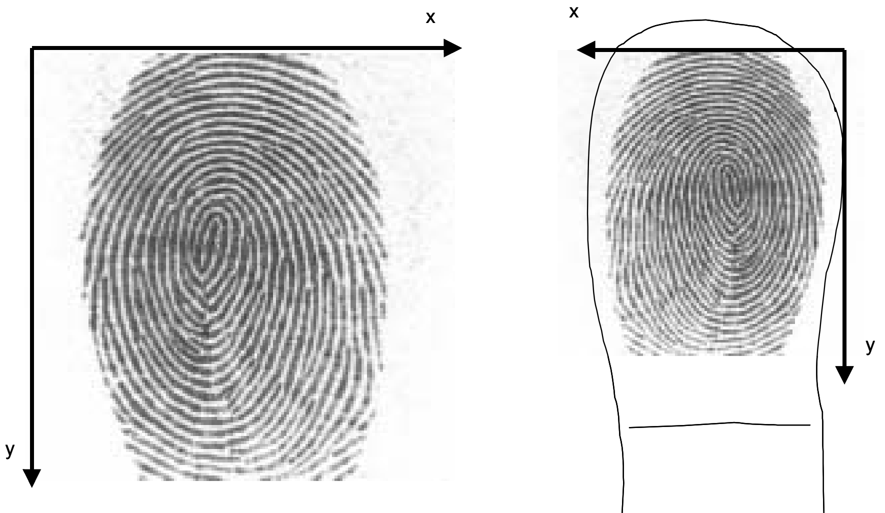


Figure 1 – Coordinate system

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).

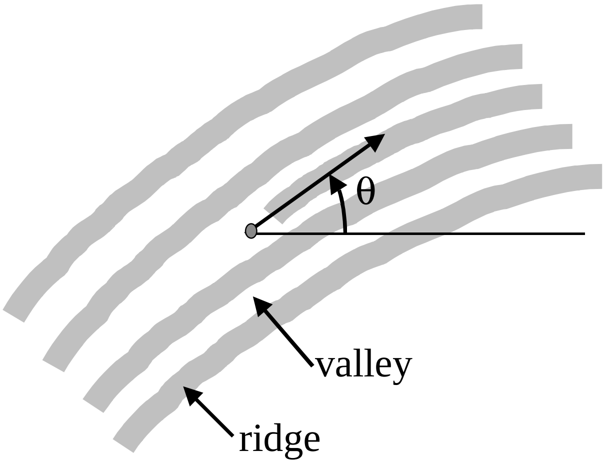


Figure 2 - Location and direction of a ridge ending (encoded as valley skeleton bifurcation point)

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).

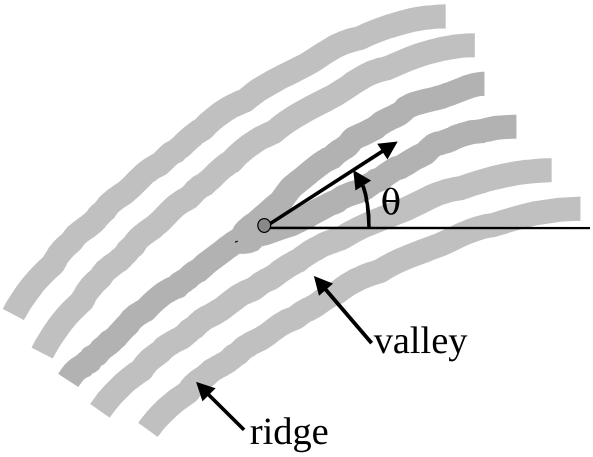


Figure 3 - Location and direction of a ridge bifurcation (encoded as ridge skeleton bifurcation point)

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).

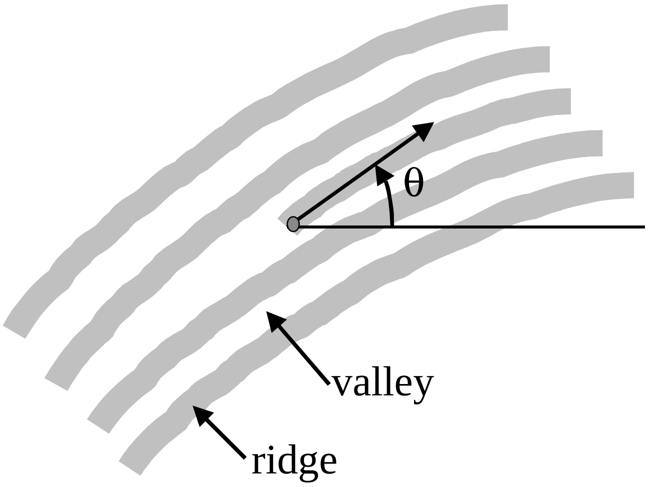


Figure 4 - Location and direction of a ridge skeleton endpoint

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.

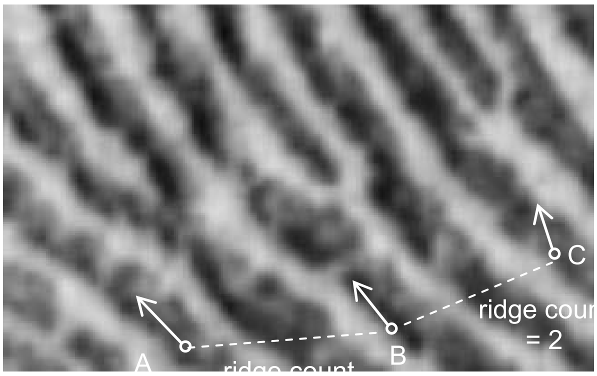


Figure 5 - Example Ridge Count data

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 (quadrants)	For each center minutiae used, ridge count data was extracted to the nearest neighboring minutiae in four 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.

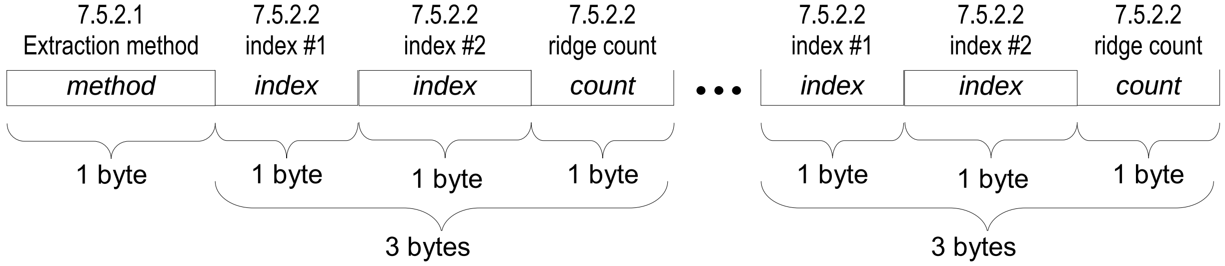
The ridge count data shall be listed in increasing order of the index numbers, as shown in Table 5. There is no requirement that the ridge counts be listed with the lowest index number first. Since the minutiae points are not listed in any specified geometric order, no assumption shall be made about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

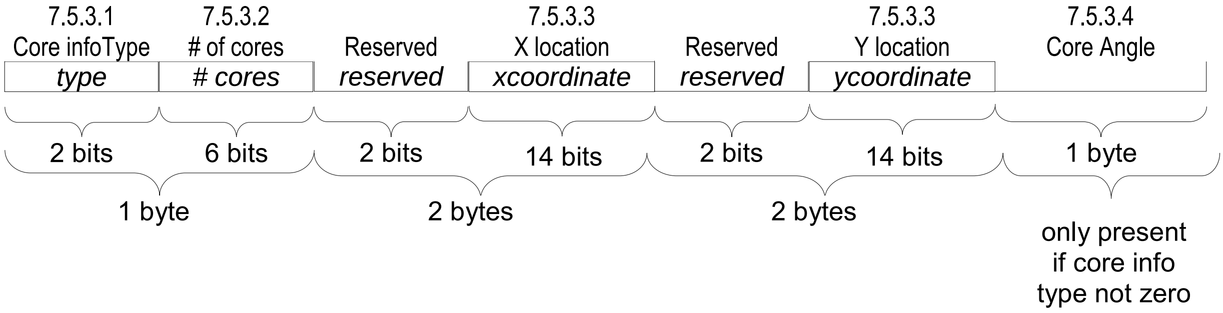
The X coordinate of the delta shall be recorded in the lower fourteen bits of the first two bytes (fourteen bits). The Y coordinate shall be placed in the lower fourteen bits of the following two bytes. The coordinates shall be expressed in pixels at the resolution indicated in the record header.

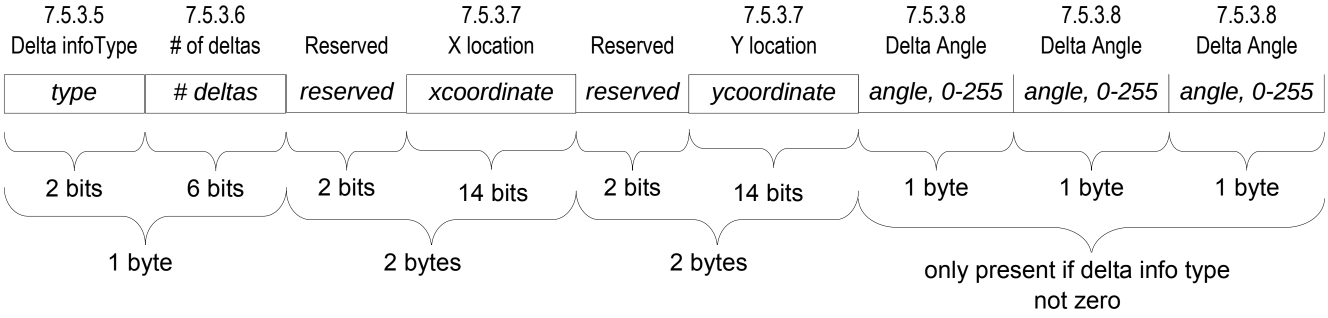
7.5.3.8 Delta Angles

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.

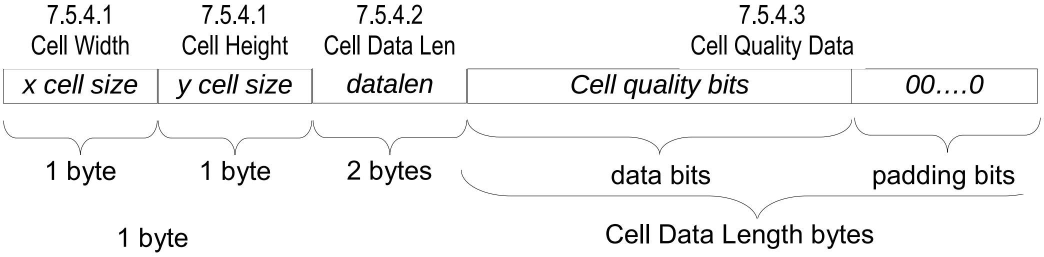
7.5.4.3 Cell Quality Data

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:



7.6 Minutiae Record 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 pe 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 = 2π/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 = 2π/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.

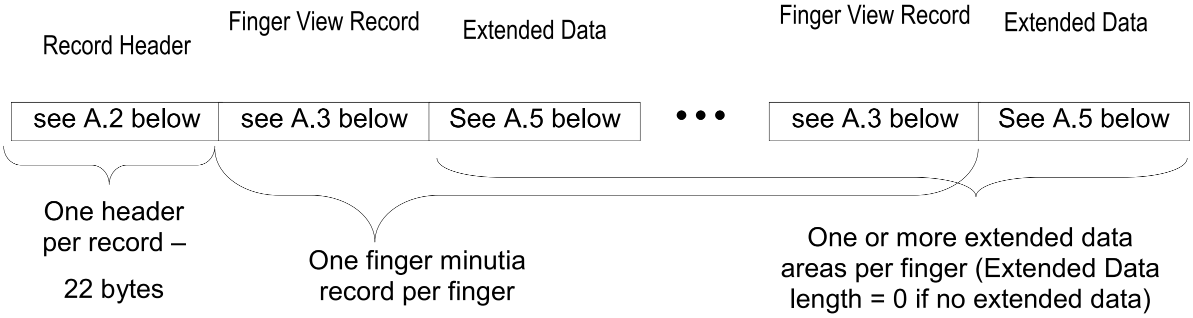
Table 18 — Format types

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



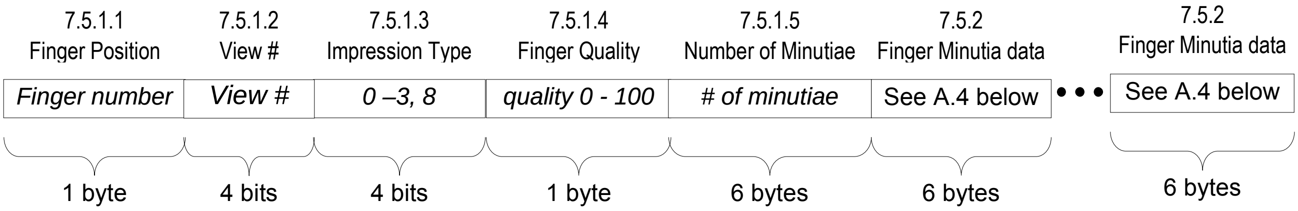
A.2 Record Header

7.4.1 Format ID	7.4.2 Spec Version	7.4.3 Record Length
`0x464D5200`	`’ ’‘X’’‘X’0`	*length*
4 bytes	4 bytes	2 or 6 bytes

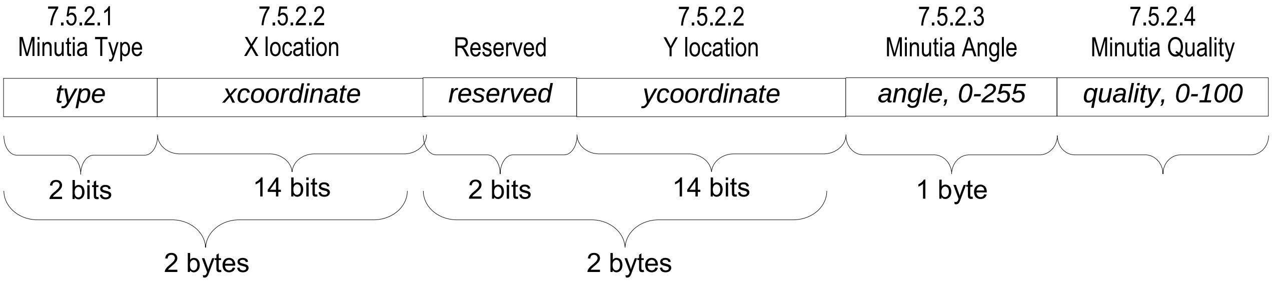
7.4.4 Capture Eqpt compliance				7.4.5 Capture Eqpt ID
Appendix F	*res'd*	*res'd*	*res'd*	*cqpt eqp ID*
4 bits				12 bits

7.4.6 X image size	7.4.7 Y image size	7.4.8 X resolution	7.4.9 Y resolution	7.4.10 # of finger views	7.4.11 Reserved byte
X image size	*Y image size*	*X resolution*	*Y resolution*	*# of views*	*0x00*
2 bytes	2 bytes	2 bytes	2 bytes	1 byte	1 byte

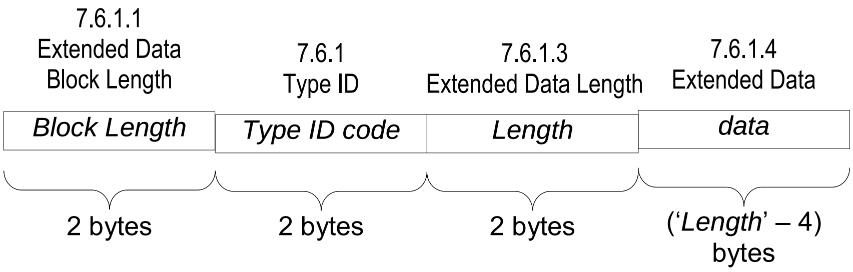
A.3 Single Finger View Minutiae Record



A.4 Finger Minutiae Data



A.5 Extended Data



Annex B
(informative)
Example Data Record

This example minutiae record demonstrates the format for a given set of data.

B.1 Data

Scanner ID = 0x00B5 (these values are determined by the IBIA - for the Vendor ID - and by the vendor)

Sensor Resolution: 500 dpi in both X and Y axes; 196.85 pixels per cm, Image was 512 by 512 pixels

Plain live-scan prints of the left and right index fingers

Left Index: Finger quality is 90% of the maximum possible; 27 minutia, listed in table below; no private feature data

Right Index: Finger quality is 70% of the maximum possible; 22 minutia, listed in table below. Private feature data area (Type 01) consisting of six bytes: 0x01, 0x44, 0xBC, 0x36, 0x21, 0x43

Record length = 340 = 26 (record header) + 2 * 4 (finger headers) + 27 * 6 (minutia for 1st finger) + 22 * 6 (minutia for 2nd finger) + 2 (null private area for 1st finger) + 10 (private area for 2nd finger)

Minutia	Left Index Finger					Right Index Finger				
#	Type	X	Y	Angle	quality	Type	X	Y	Angle	quality
0	Ending	100	14	112	90	ending	40	93	0	90
1	Ending	164	17	85	80	bifurcation	116	100	0	80
2	Bifurcation	55	18	22	90	ending	82	95	12	70
3	Bifurcation	74	22	76	60	bifurcation	140	113	15	70
4	Ending	112	22	90	80	ending	122	135	18	80
5	Bifurcation	42	31	44	90	bifurcation	55	72	21	50
6	Bifurcation	147	35	51	90	ending	94	74	24	60
7	Ending	88	38	165	40	ending	155	62	42	80
8	Bifurcation	43	42	4	80	bifurcation	42	64	55	70
9	Ending	56	48	33	70	ending	155	85	59	80
10	Ending	132	49	72	90	bifurcation	96	192	62	80
11	Bifurcation	71	50	66	80	ending	114	86	85	80
12	Other	95	51	81	90	bifurcation	142	90	90	70
13	Ending	112	53	132	50	ending	57	137	100	90
14	Bifurcation	135	58	32	80	ending	131	75	110	80
15	Other	41	60	59	70	ending	45	113	120	80
16	Bifurcation	67	62	145	90	bifurcation	111	171	130	50
17	Ending	91	63	132	80	ending	95	62	150	60
18	Ending	112	65	33	60	bifurcation	61	114	200	80
19	Ending	53	71	45	90	bifurcation	143	72	250	80
20	Bifurcation	104	74	12	80	ending	63	104	300	70
21	Ending	75	79	21	90	bifurcation	125	73	350	40
22	Bifurcation	48	80	92	90					
23	Ending	130	89	45	80					
24	Bifurcation	63	95	126	80					
25	Ending	47	108	164	90					
26	Bifurcation	126	115	172	30					

B.2 Example Data Format Diagrams

Format ID	Spec Version	Record Length	Scanner ID
0x464D5200	’0’‘2’‘0’0	*0x0000152*	*0x00B5*

X image size	Y image size	X resolution	Y resolution	# of fingers	View number
0x0200	*0x0200*	*0x00C5*	*0x00C5*	*0x02*	*0x00*
512 decimal	512 decimal	197 decimal	197 decimal	# of fingers	reserved

Finger Position	Impression Type	Finger Quality	Number of Minutiae
0x07	*0x00*	*0x5A*	*0x1B*
left index	plain live-scan	90 decimal	27 minutiae

Type & X Loc	Y Location	Minutia Angle	Minutia Quality		Extended Area Type ID
0x4064	0x000E	0x70	0x5A	• • •	*0x0000*
0x4000 (type) & 100 decimal	14 decimal	112 decimal	90 decimal		

Finger Position	Impression Type	Finger Quality	Number of Minutiae
0x02	*0x00*	*0x46*	*0x16*
right index	plain live-scan	70 decimal	22 minutiae

Type & X Loc	Y Location	Minutia Angle	Minutia Quality	
0x4028	0x005D	0x00	0x5A	• • •
0x4000 (type) & 93 decimal	93 decimal	0 decimal	90 decimal	

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

B.3 Raw Data for the Resulting Minutiae Record

Record Header:

```
0x464D520030323000015200B50200020000C500C50200
```

1st Finger Header:

```
0x07005A1B
```

1st Finger Minutiae data:

```
0x4064000E505A          0x40A400113C50          0x80370012105A
0x804A0016363C          0x407000164050          0x802A001F1F5A
0x80930023245A          0x405800267528          0x802B002A0350
0x403800301746          0x40840031335A          0x804700322F50
0x005F00333A5A          0x407000355E32          0x8087003A1750
0x0029003C2A46          0x8043003E675A          0x405B003F5E50
0x40700041173C          0x40350047205A          0x8068004A0950
0x404B004F0F5A          0x80300050415A          0x408200592050
0x803F005F5A50          0x402F006C755A          0x807E00737A1E
```

1st Private Data Area:

```
0x0000
```

2nd Finger Header:

```
0x02004616
```

2nd Finger Minutiae data:

```
0x4028005D005A          0x807400640050          0x4052005F0946
0x808C00710B46          0x407A00870D50          0x803700480F32
0x405E004A113C          0x409B003E1E50          0x802A00402746
0x409B00552A50          0x806000C02C50          0x407200563C50
0x808E005A4046          0x40390089475A          0x4083004B4E50
0x402D00715550          0x806F00AB5C32          0x405F003E6B3C
0x803D00728E50          0x808F0048B250          0x403F0068D546
0x807D0049F928
```

2nd Private Data Area:

```
0x0001000A0144BC362143
```

Annex C
(informative)

Handling of Finger Minutiae Card Formats

C.1 Enrollment

C.1.1 Number of minutiae

The number of minutiae is a security sensitive parameter and depending on the security policy of the application. Persons who do not meet the minimum required number for enrolment cannot be enrolled. The maximum number of minutiae for the reference data is implementation dependent.

The recommended minimum number of minutiae required for enrollment is 16 and for verification is 12. The strength of function (see note at the end of this clause) may have impact on these values.

The maximum number of minutiae to be sent to a card is implementation dependent and related to:

- transmission time
- memory resources
- execution time
- security aspects

The recommended maximum value for enrollment and verification is 60. It is up to the extraction device to limit the number of minutiae sent to the card to 60 or the indicated value (see CBEFF Annex G, Table G.1).

NOTE - In the Common Criteria, the following definitions are given:

Strength of Function (SOF) — A qualification of a Target of Evaluation (TOE) security function expressing the minimum efforts assumed to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic — A level of TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium — A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high — A level of TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

C.1.2 Number of required finger presentations

The number of required finger presentations during an enrollment process is enrollment system dependent.

C.2 Matching

The verification data is subject to translation (in x- and y-direction), rotation (deviation of the orientation) and distortion. Matching also has to take into account components or factors like FAR/FRR.

C.2.1 Matching conditions

The result of the matching process is a score, which may denote the number of matching minutiae or any other appropriate value. In interoperability tests, it may be verified whether different implementations of the matching algorithm meet a required FAR/FRR e.g. in relation to the strength of function for the respective application.

If minutia types are taken into account in the matching process, the different types match according to Table .

Table C.1 - Minutiae type matching

Type of verification minutiae	Match with type of reference minutiae
00	00, 01, 02
01	00, 01
02	00, 02
00 = other 01 = ridge ending (encoded as valley skeleton bifurcation point), or ridge skeleton end point, see note 02 = ridge bifurcation (encoded as ridge skeleton bifurcation point)	

NOTE – The alternatives depend on the format type.

C.2.2 Threshold Value

A verification decision result is positive (i.e. the user verification is successful), if the score S as matching result is greater or equal than the required threshold value T:

$S \geq T$

The threshold value depends on several factors or components such as

- Required False Acceptance Rate FAR
- Required False Rejection Rate FRR
- Matching conditions, see 7.2.1
- The amount of minutiae enrolled
- The amount of minutiae presented
- Strength of function.

The treatment of the threshold value is dependent on the implemented matching strategy. In the following an example of the calculation of a threshold value is presented.

The threshold value T considered in this example is a dynamic value to be calculated for each verification process and depends on:

- 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*