FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
24713-3**

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2009-05-25

Voting terminates on:
2009-07-25

Information technology — Biometric profiles for interoperability and data interchange —

Part 3:
Biometrics-based verification and identification of seafarers

Technologies de l'information — Profils biométriques pour interopérabilité et échange de données —

Partie 3: Vérification basée sur la biométrie et identification des navigateurs

Please see the administrative notes on page iii

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.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 24713-3:2009(E)

© ISO/IEC 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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

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

Violators may be prosecuted.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2009 – All rights reserved

Not for Resale

In accordance with the provisions of Council Resolution 21/1986, this document is **circulated in the English language only**.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Conformance 1

3 Normative references 1

4 Terms and definitions 2

5 Abbreviated terms 3

6 Application requirements 3
6.1 General 3
6.2 Requirements of ILO SID convention 4
6.2.1 Physical composition of the document 4
6.2.2 Personal data contained in the document 4
6.2.3 Biometric data contained in the document 4
6.2.4 Visibility of data 5
6.2.5 Secure electronic database 5
6.2.6 Restrictions on database content 5
6.2.7 Access to the database 5
6.2.8 Data protection and privacy 6
6.3 Suitable biometric modalities 6
6.4 Performance levels 6
6.5 Data storage formats and data storage media 7
6.5.1 General 7
6.5.2 Two dimensional bar code 7
6.5.3 Contactless integrated circuit 8
6.5.4 Secure electronic database 8
6.6 Security requirements 10
6.6.1 General 10
6.6.2 Protection of biometric data on the SID 10
6.6.3 Authentication of biometric data on the SID 11
6.6.4 Protection of the secure electronic database 11
6.6.5 General security requirements 11
6.7 Enrolment procedures 12
6.8 Verification procedures 14
6.8.1 General 14
6.8.2 Off-line verification procedure 15
6.8.3 On-line verification procedure 16

Annex A (normative) **Requirements list** 18
A.1 General 18
A.2 Relationship between RL and corresponding ICS proformas 18
A.3 Profile specific implementation conformance statement 18
A.4 Instruction for completing the ICS proforma 19
A.4.1 General structure of the ICS proforma 19
A.4.2 Additional Information 19
A.4.3 Exception Information 19
A.5 ICS proforma 20
A.6 Interchange formats 21
A.6.1 Finger image data (ISO/IEC 19794-4) 21
A.6.2 Finger minutia data (ISO/IEC 19794-2) 23

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2009 – All rights reserved

A.6.3 Face image data (ISO/IEC 19794-5) **25**
A.6.4 ISO/IEC 19785 (CBEFF) **28**

Annex B (normative) **CBEFF patron format for the SID** **30**
B.1 Patron **30**
B.2 Patron identifier **30**
B.3 Patron format name **30**
B.4 Patron format identifier **30**
B.5 ASN.1 object identifier for this patron format **30**
B.6 Domain of use **30**
B.7 Version identifier **30**
B.8 CBEFF version **31**
B.9 General **31**
B.10 Bit oriented patron format specification and conformance statement **31**
B.10.1 Specification **32**
B.11 Patron format conformance statement **32**
B.11.1 Identifying information **32**
B.11.2 CBEFF-defined data elements and abstract values **33**
B.11.3 Patron defined data elements and abstract values **33**

Annex C (normative) **CBEFF security block for the SID** **34**
C.1 Introduction **34**
C.2 SB owner **35**
C.3 SB owner identifier **35**
C.4 SB format name **35**
C.5 SB format identifier **35**
C.6 ASN.1 object identifier for this SB format **35**
C.7 Version identifier **35**
C.8 SB specification **35**
C.9 Size of the SB encoding **36**

Bibliography **37**

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 24713-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 24713 consists of the following parts, under the general title *Information technology — Biometric profiles for interoperability and data interchange*:

— *Part 1: Overview of biometric systems and biometric profiles*

— *Part 2: Physical access control for employees at airports*

— *Part 3: Biometrics-based verification and identification of seafarers*

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

The International Labour Organization, in response to a request from the International Maritime Organization, has adopted the Seafarers' Identity Documents Convention (Revised), 2003 (No.185). This convention requires all seafarers from ratifying nations to be issued with an identity document that follows a uniform format, has specific physical security features, and uses biometrics to link the seafarer to their identity document. Currently Convention No. 185 specifies the use of two fingerprints stored in a two-dimensional bar code, but the choice of biometric modality and storage medium could be changed provided backwards compatibility is maintained.

In order to support a globally interoperable system of Seafarers' Identity Documents (SIDs), this part of ISO/IEC 24713 establishes a biometric profile to define how to use biometrics for verification and identification of seafarers at the various stages of document issuance and inspection. It defines a set of base standards and criteria for applying those standards in applications where identity documents are issued to seafarers and biometrics are used to link each document to the seafarer to whom it was issued. It attempts to provide information on the processes surrounding the enrolment and verification or identification of seafarers so that the biometric components of the system can be used in a proper context. It also addresses other system components such as the storage medium for the biometric data and the security of the system, since these will affect the use of the biometric technology. This part of ISO/IEC 24713 is intended for use in the maritime industry, but can be applicable to other situations where identification and verification of document holders are necessary during document issuance or inspection.

The use of biometric data includes identification checks during the issuance of the document, when watchlists can be checked and the entire database of existing seafarers can be searched to prevent a single seafarer from establishing multiple identities.

It also includes the use of biometric data for verification when a card is presented at a control point by a person claiming to be the seafarer to whom the card was issued. Such control points can include port entrances, ship gangplanks, border crossing points where a seafarer must verify themselves to immigration authorities and any other situation where the seafarer needs to verify their identity as a seafarer. This verification is expected to be performed not only indoors under controlled conditions, but also outdoors in difficult conditions, including harsh wet weather, salt spray, high humidity and high temperatures. Biometric equipment and credentials have to be capable of functioning in all such environments.

This part of ISO/IEC 24713 is not intended in any way to conflict with the existing international Convention No. 185 established by the International Labour Organization and ratified by various member states of the ILO. Instead, the approaches profiled in this part of ISO/IEC 24713 can be used to satisfy the requirements of the current version of Convention No. 185 while also allowing alternative approaches outlined in this part of ISO/IEC 24713 to be used in the future by the ILO if the technical documents associated with or annexes of Convention No. 185 are modified. To this end, the concept of backwards compatibility is stressed. The fundamental choices already made by the ILO of the use of a minutiae-based, two-finger template for seafarer verification, of the inclusion of a photograph and signature in the visible area of the SID, and of the use of a two-dimensional barcode as a storage medium are respected in this profile. Where alternative technology choices are promoted, they are defined in such a way that there will still be backwards compatibility with existing SIDs.

This part of ISO/IEC 24713 defines a CBEFF patron format in Annex B and a CBEFF Security Block in Annex C that are suitable for the limited storage available in a two dimensional barcode and which may be relevant for other storage constrained environments.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Information technology — Biometric profiles for interoperability and data interchange —

Part 3:
Biometrics-based verification and identification of seafarers

1 Scope

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

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

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

2 Conformance

All seafarers' identity documents, systems used for issuing seafarers' identity documents, and systems used for verification or identification of seafarers that claim conformance to this part of ISO/IEC 24713 shall conform to the mandatory requirements of Clause 6 of this part of ISO/IEC 24713 and of the normative Annexes referenced therein.

3 Normative references

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

ISO/IEC 7501-1, *Identification cards — Machine readable travel documents — Part 1: Machine readable passport*

ISO/IEC 7501-3, *Identification cards — Machine readable travel documents — Part 3: Machine readable official travel documents*

ISO/IEC 8824-1:2002, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

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)*

ISO/IEC 8825-2:2002, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 15438:2006, *Information technology — Automatic identification and data capture techniques — PDF417 bar code symbology specification*

ISO/IEC 19785-1:2006, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-2:2005, *Information technology — Biometric data interchange formats — Part 2: Finger minutiae data*

ISO/IEC 19794-4:2005, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5:2005, *Information technology — Biometric data interchange formats — Part 5: Face image data*

ISO/IEC 19795-4:2008, *Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing*

ISO/IEC 24713-1:2008, *Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles*

ISO/IEC 29109-1, *Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24713-1 and the following apply.

NOTE There are some terms which are commonly used in this part of ISO/IEC 24713 but are not explicitly defined. Specifically, verification authority, issuing authority, competent authority and focal point are terms which address legal entities that are the responsibility of the ILO and which vary from country to country. These terms are used frequently in ILO Convention No. 185 but their precise definition is best left to the interpretation of ILO legal experts. Further explanations can be found by reading Convention No. 185 as provided in the bibiliography or by consulting with the ILO.

4.1
biometric characteristic
measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrolee

4.2
biometric enrolment
process of creating and storing, for an individual, a data record associated with an individual and including biometric reference(s) and, typically, non-biometric data

4.3
biometric feature
concise representation of information extracted from an acquired or intermediate biometric sample by applying a mathematical transformation

4.4
biometric model
stored function (dependent on the biometric data subject) generated from a biometric feature(s)

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.5
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

4.6
enrolee
person who has a biometric reference template recorded for the purpose of issuing a SID

4.7
IC chip
processor and storage embedded in a SID that contains information suitable for verification of the seafarers' identity when read by a SID verification station that is equipped to communicate with an IC chip

NOTE This is also called a contactless integrated circuit.

4.8
seafarer
person who is employed or is engaged or works in any capacity on board a vessel (other than a ship of war) ordinarily engaged in maritime navigation

4.9
Seafarers' Identity Document
SID
document containing identifying information about a seafarer including demographic information, a photo of that seafarer and biometric data contained within a PDF 417 bar code or optionally an IC chip

NOTE It is expected that in initial deployments of SIDs the inclusion of an IC chip will be optional but that more deployments will migrate to that technology as IC chips and the technology to perform biometric verification using IC chips become ubiquitous.

4.10
SID verification station
system of hardware and software that supports the biometric verification of a seafarer's identity using information recorded on the SID, optionally including the capability to perform on-line verification of the SID with a secure electronic database provided by the issuing authority that issued the SID

NOTE A single verification authority will often support multiple SID verification stations, some of which may be required to function on board ships or in other difficult environments where no on-line access is available.

5 Abbreviated terms

CBEFF Common Biometric Exchange Formats Framework

ILO International Labour Organization

SID Seafarers' Identity Document

6 Application requirements

6.1 General

The requirements of a globally interoperable system of seafarers' identity documents to be used for the biometric verification and identification of seafarers are outlined in this clause. The requirements focus on the biometric aspects of this application, but where other aspects affect the use of biometrics, they are also discussed. These requirements are intended to be in accordance with the regulatory requirements of the Seafarers' Identity Documents Convention (Revised), 2003 (No.185) [3] and to ensure backwards

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

compatibility with the existing practices of the ILO and with SIDs already issued. There are currently several requirements of the existing Convention that would be difficult to change and which this standard normatively requires for all verification and identification of seafarers. Permission has been given for certain portions of Convention No. 185 to be quoted directly in this document, and these are used to help define the requirements. The relevant sections of Convention No. 185 (renumbered to make sense when quoted without the full text of the Convention) follow in Clause 6.2.

6.2 Requirements of ILO SID convention

6.2.1 Physical composition of the document

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

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

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

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

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

6.2.2 Personal data contained in the document

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

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

b) sex;

c) date and place of birth;

d) nationality;

e) any special physical characteristics that may assist identification;

f) digital or original photograph; and

g) signature

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

6.2.3 Biometric data contained in the document

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

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

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

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

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

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

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

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

6.2.4 Visibility of data

All data concerning the seafarer that are recorded on the document shall be visible. Seafarers shall have convenient access to machines enabling them to inspect any data concerning them that is not eye-readable. Such access shall be provided by or on behalf of the issuing authority.

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

6.2.5 Secure electronic database

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

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

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

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

6.2.6 Restrictions on database content

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

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

6.2.7 Access to the database

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

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

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

6.2.8 Data protection and privacy

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

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

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

6.3 Suitable biometric modalities

Although many biometric modalities are suitable for use with seafarers, current practice uses two fingerprints, preferably one from each hand. These fingerprints are stored in a single template with two finger views, formatted in accordance with the card normal format (including a record header) defined by an early draft of ISO/IEC 19794-2 and profiled in detail in ILO SID-0002 [4]. Any other modalities selected should therefore be used in addition to a minutiae based fingerprint template in order to maintain backwards compatibility.

Since existing practice for seafarers' identity documents is to show a photograph of the seafarer’s face on the printed document, it is current practice to collect both fingerprints and facial images for most seafarers. All applications for biometric verification and identification that are conformant to this standard shall use fingerprint as a mandatory biometric and face as an optional additional biometric.

6.4 Performance levels

The International Labour Organization has already specified a performance level that it deems to be acceptable for verification of seafarers at ports and on board ships. It has not, however, specified a performance level for identification of seafarers which may be relevant during background checks or duplicate issuance checks when the seafarer is being enrolled into one of the electronic databases described in 6.2.5 and having their identity document issued. Given the dependence of the identification performance on the quality of the input biometric data and the lack of detailed performance testing methodology standards for identification operations, the simplest solution is to adopt the current ILO specified performance levels as the minimum performance levels.

Biometric systems that perform enrolment or verification functions for use with seafarers, as defined by this profile, shall be able to achieve specified metrics of interoperable performance (as defined by ISO/IEC 19795-4) that are measured using generalized transactional false accept rate (GFAR) and generalized transactional false reject rate (GFRR). Specifically the mean interoperable GFRR at a GFAR of 1 % shall be less than 1 % for all systems in an interoperable group and the maximum GFRR at a GFAR of 1 % for any combination of enrolment system and verification system shall be less than 2 %. Interoperable groups may be defined such that systems may be either enrolment only or verification only or both.

Any tests to determine which biometric systems meet the interoperable performance thresholds mandated by this standard shall be conformant to ISO/IEC 19795-4.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.5 Data storage formats and data storage media

6.5.1 General

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

For these reasons, the format for storing fingerprints in a seafarers' identity document shall be one of those defined in ISO/IEC 19794-2.

Since existing practice is to display photographs on seafarers' identity documents, there should not be any privacy issues with using face images. Therefore the storage format for face images shall be ISO/IEC 19794-5.

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

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

6.5.2 Two dimensional bar code

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

For ID-3 size booklets, the bar code shall be placed immediately to the right of the printed photograph of the seafarer (Zone V in ISO/IEC 7501-1) and immediately above the machine readable zone (Zone VII in ISO/IEC 7501-1). In order to leave space for other necessary data elements the area allotted for the two dimensional bar code including all necessary quiet zones shall not be more than 21,35 mm in height and it shall not extend below 23,2 mm above the bottom of the document since the first 23,2 mm are allotted to the machine readable zone. The bar code shall also be limited in width by the end of the printed photograph in Zone V on the left side and the 2 mm no-print zone at the edge of the document on the right side. Since the width of the photograph is somewhat flexible in ISO/IEC 7501-1, it is not possible to specify an exact width for the bar code.

For ID-1 size cards, the bar code shall be printed on the reverse side of the card from the printed photograph and shall be printed at the top of this side of the card, with the machine readable zone printed at the bottom. The two dimensional bar code shall be printed entirely within Zone VI as defined in ISO/IEC 7501-3 and therefore the maximum size of the two dimensional barcode shall be 85,6 mm in width and 27,8 mm in height including all necessary quiet zones.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

The data contained within the two dimensional barcode shall be encoded and printed using the PDF 417 bar code symbology specification defined in ISO/IEC 15438. The precise size of the bar code data symbols as well as the number of rows and columns should be decided by the authority that prints the document based on the size of the document and the print technology used to create it. The only mandatory requirement is that an error correction level of 5 shall be used and the barcode shall be readable with commercial hand held barcode readers. One recommended option is to use an x-dimension for the bar code data symbols of 0,170 mm and a y-dimension of 0,511 mm.

6.5.3 Contactless integrated circuit

If the SID also contains a contactless integrated circuit, then it shall respect the provisions of Clause 6.2. Specifically, it shall not contain any information pertaining to the seafarer other than that listed in Clauses 6.2.2 and 6.2.3 and this information shall be visible somewhere else on the document (such as the photo or demographic data printed on the document or the fingerprints stored in the bar code on the document). The contactless integrated circuit is not constrained by the storage capacity limits of the bar code, however, and there is more flexibility in the specific CBEFF format types that may be used.

The integrated circuit shall contain fingerprint data consisting of a two finger minutiae record that is conformant to either CBEFF format type 3 or 4 as defined in ISO/IEC 19794-2 and profiled in Clause A.6.2 of this standard. The integrated circuit shall also contain face image data comprising a digital representation of the photograph printed on the document, stored in a data record that is conformant to ISO/IEC 19794-5 as profiled in Clause A.6.3 of this standard. The finger minutiae data record shall be encapsulated in a CBEFF data record specified in Annex B and profiled in Clause A.6.4 of this standard. As in the case of the two dimensional bar code, a security block shall be mandatory and shall contain a digital signature of the biometric data using the method outlined in Clause 6.6 of this standard.

Finger image data, as defined in ISO/IEC 19794-4 and profiled in Clause A.6.1 of this standard shall not be stored in the contactless integrated circuit, but is restricted to use in the secure electronic SID database of an ILO member state.

Since the use of the contactless integrated circuit is optional and not mandatory, the precise specification of the data blocks stored in the IC chip is not provided here. It is recommended that the chip follow the specification for an ePassport containing face image and finger minutiae data, but it is expected that ILO will make the final decision on that and publish additional documentation to define the specification after consultations with other relevant bodies such as the International Civil Aviation Organization. As such, this is beyond the scope of this part of ISO/IEC 24713.

6.5.4 Secure electronic database

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

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

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

Item No	Data Element	Data Description	Mandatory or Optional	Present in Legacy SID Electronic Databases
1	Issuing authority named on the identity document	Variable Length Text String containing the three character ISO code (see ISO/IEC 7501-1) for the issuing state and the name and full address of the SID issuing authority as well as the name and position of the person authorizing the issue	Mandatory	Yes
2	Full name of seafarer as written on the identity document	Variable Length Text String containing the full name of the seafarer	Mandatory	Yes
3	Unique document number of the identity document	12 Character Text String containing the three character ISO code (see ISO/IEC 7501-1) for the issuing state followed by a nine character document identity number that is unique among all SIDs issued by the SID issuing authority in that state	Mandatory	Yes
4	Date of expiry or suspension or withdrawal of the document	10 Character Text String (ASCII encoded) containing a date of expiry, suspension or withdrawal of the document in the format (dd/mm/yyyy)	Mandatory	Yes
5	Status of document termination date	1 Character Text String (ASCII encoded) indicating the meaning of the date field described in data element 4. This is set to: D – Date is date of expiry of document S – Date indicates date on which document was suspended W – Date is date on which document was withdrawn	Mandatory	No
6	Fingerprint template appearing on the identity document	Variable Length Binary containing the two fingerprint ISO/IEC 19794-2 minutiae record encapsulated in a CBEFF record containing a security block exactly as encoded in the two dimensional barcode in the SID and described in Clause 6.5.2 of this standard.	Mandatory (unless prohibited by legislative requirements)	Yes May be in ISO/IEC 19794-2 format profiled in ILO SID-0002

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7	Face image appearing on the identity document	Variable Length Binary containing the facial image that is printed as the photograph on the physical SID contained within a ISO/IEC 19794-5 face image record as profiled in Clause A.6.3 of this standard and using a CBEFF header and Security Block as profiled in Clause A.6.4 of this standard.	Mandatory	Yes May be simple image without ISO/IEC 19794-5 format
8	Fingerprint images corresponding to the minutiae record of two fingers stored in the identity document'	Variable Length Binary containing the two fingerprint images that correspond to the two fingers present in the minutiae record present in the two dimensional barcode on the document. These images shall be encoded in a single ISO/IEC 19794-4 fingerprint image record as profiled in Clause A.6.1 of this standard.	Optional	No
9	Details of all inquiries made concerning the seafarers' identity document	Internal database logs recording the identity of the verification authority making each inquiry, the details used to validate that verification authority, the date and time of the query and the unique document number of the SID against which the enquiry was made. The internal format used to record this information is up to each issuance authority as this information is not for exchange but for providing audit reports to issuance authorities and, for queries against their own SID, to seafarers.	Mandatory	Yes

Table 1 — Data Elements in the Secure Electronic Database

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

6.6 Security requirements

6.6.1 General

There are three fundamental security issues that are relevant to the verification and identification of seafarers and that are addressed in this standard.

6.6.2 Protection of biometric data on the SID

The face image data that shall be stored on the contactless integrated circuit if one is present on the SID has the same information content as the printed photograph. Therefore no cryptographic data protection is required.

The finger minutiae records are typically considered to be more sensitive, but based on existing ILO policy it appears that minutiae records do not need cryptographic protection against reading, provided that they can't be read unless the card is voluntarily surrendered by the seafarer.

In the case of the minutiae record stored in the bar code, in normal operation of verifying the identity of the seafarer, the record will be scanned once the seafarer voluntarily surrenders the document so that the bar code can be scanned. Only in exceptional circumstances, such as the legal confiscation of an SID or a seafarer losing an SID, would it be possible for the barcode to be scanned without the seafarers' permission.

In the case of the minutiae record that shall be stored on the contactless integrated circuit if one is present on the SID, the simplest solution is to use the Basic Access Control (BAC) method that is commonly used for ePassports. Therefore, the biometric data stored on the SID is not encrypted, but if a contactless integrated circuit is present, access to it shall be protected using the Basic Access Control method that is commonly used for ePassports.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.6.3 Authentication of biometric data on the SID

In order to prevent fraud, it is necessary to ensure that the biometric data stored on the SID actually matches the biometric characteristics of the seafarer and that the data was encoded and the document created by a trusted SID issuing authority. One method of doing this is to access the secure electronic database of the issuing authority and verify the authenticity of the SID. Since many SID verification stations may be located in ports or on ships where there is no availability of a communication infrastructure to access the electronic databases of all SID issuing authorities, there must be an immediate method of authenticating the SID.

The method that shall be employed is to use the digital signature contained in the CBEFF security block. Since the cryptographic functions relate only to the digital signature (encryption of a hash), the related keys, algorithms and parameters used to validate the digital signature do not need to be kept secret, but their origin has to be ensured. Ideally, once the globally unique document number has been obtained from the SID, the necessary parameters to validate the digital signature (and hence the biometric data) can be obtained on-line using a PKI secured infrastructure from a trusted third party such as the ILO.

Where on-line access via a PKI secured infrastructure is not available to obtain these parameters (and any revocation information), the verification station should download and store the algorithms and parameters from the trusted third party when on-line access becomes available. The stored information should be refreshed no less frequently than once a month.

The SID includes in the machine readable zone and in the CBEFF Security Block of each biometric data record stored on the document, a 12 character globally unique document number identical to that stored in the secure electronic database and described in Table 1 above. The downloaded information shall contain (for each issuing authority, and for each group of SID numbers designated by that issuing authority to require a separate public key) the parameters and public key used for the message digest and the digital signature that were used by that issuing authority when producing that group of SIDs. The downloaded information shall also contain a list of the unique document numbers of any cards issued during that month that have been revoked.

The simplest way to manage secure distribution of this information is by using either a single global focal point coordination centre (as proposed for on-line verification in Clause 6.8.3) or to use a simplified public key infrastructure such as the ICAO Public Key Directory being used for ePassports. The definition of such a mechanism lies beyond the scope of this standard, but the details presented in this Clause are essential to the successful operation of such a system.

NOTE These parameters need not be kept secret, but they need to be obtained from a trusted source, otherwise the verification authority may fail to detect fraudulent cards by use of parameters and a public key obtained from the issuer of the fraudulent card. Thus any downloaded list stored in the SID verification station needs to be protected from tampering (by physical means).

6.6.4 Protection of the secure electronic database

In order to protect the data contained in the secure electronic database, it is important that IT security best practices be followed. These are beyond the scope of this document, but include such matters as limiting access to the database only to authorized personnel, recording all access requests and changes made to the database in audit logs and ensuring a regular review of such audit logs. The database must only be accessible to verification authorities following the procedures outlined in Clause 6.8 and any data shall only be transmitted to properly authenticated verification authorities and shall be protected during transit.

6.6.5 General security requirements

There are numerous security requirements that are common to all biometric applications and these should be followed in biometric verification and identification of seafarers. It is not appropriate to repeat all of them in this standard, but a few key concepts are repeated for the benefit of implementers of the standard.

The biometric capture devices used should be resistant to the harsh environmental conditions, including salt spray, found in ports and on board ships, while still retaining enough discriminating power to make spoofing difficult.

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The verification of seafarers should include a step to verify the authenticity of the SID, either by checking with the secure electronic database or by verifying the digital signature in the CBEFF security block for the biometric data being used to verify the seafarer.

The biometric enrolment and verification systems should be designed so that it is difficult to insert data into the system or siphon data from the system through illegitimate channels. This will protect the integrity of the issuance process and protect against replay attacks and man in the middle attacks on the verification system.

Once a system component in the enrolment or verification systems has completed its function, the data used by that component should no longer be accessible in that component. For example, the biometric capture device should clear its memory after a capture sequence is complete and the Matching and Comparison component(s) should clear biometric data from memory after a match score is computed and a match decision rendered.

These are only a few of the elements of general information security best practices. It is recommended that the practices outlined in detail in the bibliography references [5], [6] and [7] should be followed where possible and provided they do not conflict with any of the specific requirements of this part of ISO/IEC 24713.

6.7 Enrolment procedures

Each SID issuing authority shall verify the eligibility of the individual applying for a seafarers' identity document. This may include checking that the individual is a qualified seafarer using national training records, employment records or other sources. It may also include verifying the identity and nationality of the seafarer through the use of breeder documents and existing national databases. These processes may vary from one SID issuing authority to another, since available documents and databases will vary from one nation to another, as will regulatory requirements.

There are certain procedures during the process of issuing a seafarers' identity document that will be common among all issuing authorities. Specifically, the issuing authority will need to obtain the demographic and biometric data of the seafarer and enter them into the issuance system so that they can become part of the secure electronic database and be included on the SID, assuming one is issued for that seafarer. The demographic data recorded shall be sufficient to produce the SID, including the machine readable zone, as specified in ISO/IEC 7501-3. As a minimum, the demographic data recorded shall include the following:

a) primary identification – the seafarer's primary identifying name;

b) secondary identification – the seafarer's secondary identifying name;

c) nationality – a three letter country code (see ISO/IEC 7501-1) representing the seafarer's nationality;

d) place of birth – the seafarer's place of birth;

e) date of birth – the seafarer's date of birth, recorded under the Gregorian Calendar as year, month and day; and

f) gender – the gender of the seafarer.

The biometric data of the seafarer shall be captured in an enrolment process that takes place as part of the overall process of issuing and producing an identity document, in this case an SID.

The enrolment shall include the capture of a face image that meets the criterion for a full frontal (Face Image Type = 1) image as defined in ISO/IEC 19794-5 and the encoding of it into an ISO/IEC 19794-5 conformant record as defined in Clauses 6.5.3 and 6.5.4. The enrolment shall also include the capture of at least two fingers, which may optionally be stored in the secure electronic database as ISO/IEC 19794-4 conformant finger image records and which shall have minutiae extracted to create an ISO/IEC 19794-2 conformant finger minutiae record to be stored mandatorily in the secure SID database (unless prohibited by legislative requirements) and mandatorily on the SID.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In the enrolment of both face and fingerprint biometrics, the SID issuing authority (or their enrolment office) should take particular care to obtain high quality images in order that the verification of the identity of seafarers by SID verification authorities (see Clause 6.8) is facilitated. The capture of a poor quality fingerprint image can result in a set of recorded minutiae for that finger which fails to match sufficiently the set of minutiae obtained on processing of the finger images at verification. SID issuing authorities may be able to request suppliers of biometric enrolment equipment to provide training materials on how to collect the best possible images. Examples of issues to consider during fingerprint enrolment include:

- Controlling temperature, humidity and lighting levels of the environment in which enrolment takes place in accordance with recommendations from equipment suppliers;
- Positioning of the fingerprint sensor at an optimal height and angle;
- Monitoring and responding to excessive moisture or dryness of the seafarer's finger;
- Feedback to the seafarer in correct placement of the flat part of the finger (as opposed to the finger tip) in contact with the platen, and in applying sufficient pressure;
- Ensuring that the seafarer’s finger is not excessively rotated on the platen of the sensor;

Quality control procedures should be developed to track conformance with enrolment best practices by individual enrolment officials (and by different offices, if more than one enrolment office is used by a SID issuing authority). Periodic reports should evaluate this conformance and make recommendations if there are issues in consistently obtaining high quality fingerprints during enrolment.

The decision of which two fingers to capture for this purpose is made by attempting to enrol the fingers of the seafarer in the order specified below. If a finger is unable to be enrolled because of poor quality or because the seafarer is unable to present a fingerprint (perhaps due to physical disability or damage to the finger) then the next finger in the list is enrolled in its place.

In the two finger minutiae records stored in both the database and the SID, the first finger is the first one in this list to be successfully enrolled and the second finger is the second one in this list to be successfully enrolled.

Recommended practice is to allow three finger placements to be used to enrol each finger and only to move to the next finger if all three are of insufficient quality. Prior to the completion of the enrolment process, it is also recommended to allow the seafarer to verify both of the selected fingers and if verification is not successful to move on and choose alternate fingers from the list.

a) right index finger

b) left index finger

c) right thumb

d) left thumb

e) right middle finger

f) left middle finger

g) right ring finger

h) left ring finger

i) right little finger

j) left little finger

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Biometric systems are neither completely accurate nor accessible to all. People with unreadable fingerprints, for example, have the same need for dignity and security as others. In order to address this, there needs to be a fallback procedure for those who can't enrol any two fingers from the above list. The solution is to create a finger view that represents a finger that could not be enrolled. If the seafarer can only enrol a single finger from the list above, then that finger shall be encoded in the first view of the two finger minutiae record and the second finger view shall be encoded in the profiled manner described in Annex A but with specific items having the fixed values shown in Table 2. If no finger can be enrolled, then both finger views in the ISO/IEC 19794-2 conformant record shall be encoded in the profiled manner described in Annex A but with specific items having the fixed values shown in Table 2. This allows a seafarer who is unable to use fingerprints to be issued a valid and digitally signed SID card. When a verification authority encounters such an SID card, they will know it was issued this way for valid reasons and can use the secure electronic database of the relevant SID issuing authority to verify the seafarer, although this will require that the SID verification station has on-line access.

Of course most seafarers will not have a problem enrolling the right and left index fingers, and the SID issuing authority may, depending on local legislation and practice, want to enrol all of their fingerprints to assist in identification checks against biometric databases of persons of interest to competent authorities or to prevent duplicate issuance of multiple SIDs to the same individual. As described in Clause 6.5.4, any additional fingerprints stored beyond the first two to be successfully enrolled from the list above shall not be stored in the secure electronic database.

Item	Section	Status	Operator	Operand
12	Finger Position	M	EQ	0
13	View Number	M	EQ	0
14	Impression Type	M	EQ	0, 1, 8
15	Finger Quality	M	EQ	0x65 – If fingers could not be enrolled due to seafarer disability 0x66 – If fingers could not be enrolled due to poor quality
16	Number of Minutiae	M	EQ	0

Table 2 — The Characteristics of the Unenrolled Finger

6.8 Verification procedures

6.8.1 General

SID verification authorities may wish to verify seafarers at ports, on board ships prior to the arrival of the ship in a port, and at other border crossing points where seafarers may be transiting to join or leave their ships.

In some cases, the verification authority will have on-line access to an internet link to the secure electronic database of the issuing authority that issued the SID being presented by the seafarer who is being verified. In other cases, it will not. Therefore the verification procedure is defined to use an off-line process first that relies only on the SID and cached data for the biometric verification of the seafarer. Where it is convenient, or where the SID verification authority believes that additional authentication of the seafarer is absolutely necessary, the on-line procedure may also be used.

All SID verification systems claiming conformance to this standard shall support the off-line verification procedure described in Clause 6.8.2. They may optionally support the on-line verification procedure described in Clause 6.8.3. Since there will be circumstances when those verification systems that support the on-line verification procedure will seek to use it with seafarers from any specific nationality, all secure electronic databases claiming conformance to this standard shall support the on-line verification procedure described in

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Clause 6.8.3. A manual fallback procedure may optionally be supported for special circumstances in which no internet connection is available, but such a manual procedure would necessarily involve bilateral arrangements between the verification authority and the issuing authority in question so that the focal point of that issuing authority could properly authenticate the identity of the verification authority before providing information about any seafarers in its secure electronic database. Such bilateral arrangements are not within the scope of this standard.

6.8.2 Off-line verification procedure

Any system for verification of seafarers that claims conformance to this standard shall be used in a supervised fashion and shall support the functions listed below.

a) Read the PDF 417 bar code printed on an SID as described in Clause 6.5.2 and specified in ISO/IEC 15438 and decode the ISO/IEC 19794-2 conformant two finger minutiae record stored on that bar code.

b) Verify the authenticity of the fingerprint data by checking the digital signature of the ISO/IEC 19794-2 record, and display the result of whether or not the signature can be authenticated. This will require the authenticated public key of the SID issuing authority to be known by the SID verification station.

c) If both fingers stored in the bar code are unenrolled fingers (see Clause 6.7 above), then indicate this so that the verification authority representative can take appropriate action. If not, then prompt the seafarer either visually or audibly for the first finger stored in the ISO/IEC 19794-2 finger minutiae record (usually the right index finger) to be placed on the fingerprint capture device.

d) Capture the fingerprint from the finger placed on the device by the seafarer and attempt to match it with the first finger stored in the ISO/IEC 19794-2 conformant finger minutiae record extracted from the bar code.

e) If the finger placed does not match the finger minutiae record extracted from the bar code using a threshold established in independent testing to achieve the interoperable performance required in Clause 6.4, then allow a total of three placement attempts before prompting for the second finger stored in the ISO/IEC 19794-2 conformant minutiae record. If this second finger is an unenrolled finger (See Clause 6.7 above), then do not prompt for it to be placed, but instead indicate this so that the verification authority representative can take appropriate action.

f) If the second finger also fails to match during three separate placement attempts (for a total of six finger placements), then indicate that the seafarer could not be verified so that the verification authority representative can take appropriate action.

g) If either the first or second finger produced a match score above the threshold on any of their respective placement attempts, then indicate that the seafarer was successfully verified and do not prompt for any more finger placements.

A verification system may also support the optional off-line functions listed below.

h) Read the machine readable zone (MRZ) from the SID and use the data to simplify looking up the correct public key for digital signature verification, to populate a verification authority database or to implement Basic Access Control for a contactless integrated circuit present on the SID.

i) Using Basic Access Control, access an IC chip on the card, if one is available and read an ISO/IEC 19794-2 conformant finger minutiae record and/or an ISO/IEC 19794-5 conformant face image record. The finger minutiae record may be used for fingerprint verification of the seafarer exactly as described above. The face image data may be used for facial recognition verification of the seafarer or for simple visual display by the verification system.

j) Capture an image of the seafarer's face and compare it to the ISO/IEC 19794-5 conformant face image record. The number of capture attempts and the performance levels are not specified in this part of ISO/IEC 24713, since verification using face recognition is not the primary means of biometric verification of seafarers.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

k) If the seafarer's face matches the ISO/IEC 19794-5 conformant face image record beyond a threshold specified in the security policy of the verification authority, then indicate that the seafarer has been verified using face recognition.

6.8.3 On-line verification procedure

The on-line verification procedure requires that the verification authority has access to the internet and that it has been given remote access rights to the secure electronic database of the issuing authority corresponding to the SID being verified. A single global focal point coordination centre shall manage access rights for all SID verification authorities and for the focal points maintained by all SID issuing authorities. Standard procedures for issuing and transferring certificates to grant each verification authority and each issuing authority the necessary access to a secure server maintained by the focal point coordination centre and to grant this server access to the secure electronic databases maintained by each focal point shall be followed.

After the SID verification authority has authenticated itself to the focal point coordination centre server, it shall be given access to a secure web page or other equivalent mechanism on that central server. This web page shall permit the verification authority to make enquiries about single SIDs or about groups of SIDs by uploading manifest files containing the available information about those SIDs. The focal point coordination centre server shall then forward the enquiry to the server connected to the secure electronic database of the appropriate focal point or focal points and accumulate the responses to form a combined response for all SIDs involved in the enquiry. It shall display the results to the verification authority and also allow the results to be downloaded in an enquiry result file. Since there are multiple types of queries, as described below, the verification authority will need to select on the secure web page of the focal point coordination server exactly which type of query is desired. Also, since some data elements in the secure electronic database are optional, it is possible that a combined enquiry generated by uploading a manifest file shall contain certain requested data elements only for a subset of the seafarers included in the original manifest. The structure of the enquiry result file shall therefore be flexible enough to accommodate this. Also, since local privacy legislation may restrict the data that some focal points are able to release, the focal point coordination server system shall support permissions such that each focal point can decide which, if any, of the optional data elements they will release to each ILO member state that may submit an enquiry.

The different types of enquiry outlined below assume that the verification authority has either received items 1 through 4 from Table 1 in advance of the seafarer’s arrival (which is a requirement of ILO Convention No. 185) or has obtained them directly from the SID presented by the seafarer upon their arrival. If the items were transmitted in advance, such as when a ship is preparing to dock at the first port in a new country, then the manifest file submitted may contain information on all the seafarers from that vessel and it is highly recommended that verification authorities request that information about arriving seafarers be sent to them using the same manifest file format as they will use when submitting enquiries. Thus, all enquiries require the verification authority to provide items 1 through 4. In all cases, the focal point shall respond with a verification of whether the four data elements are correct. This can be a simple “Yes” or “No” answer, but the focal point shall also respond with the correct value for each of the four items submitted and with item 5, or with a message that no matching SID was found. Since scanning errors or typos could result in some of the text strings being incorrect in the enquiry made by the verification authority, it is recommended that the focal point use the SID number as the primary key and if that fails, then attempt a search based on the name of the seafarer and the date of expiry of the SID.

Additional data elements requested beyond the simple response and correction of items 1 through 4 may include the face image, the fingerprint template or the fingerprint image. For those focal points that do not wish to disseminate the fingerprints of their seafarers, but are willing to support a biometric matching service on their focal point server, the enquiry may also submit fingerprint templates. This type of enquiry could only happen when a seafarer was present as they would have to submit their fingerprints to a verification authority device so that they could be captured and have an ISO/IEC 19794-2 minutiae template extracted and included in a manifest file to be uploaded to the focal point coordination centre server. Since this process would be rather cumbersome, it is permitted, but not recommended for general use. It may be applicable for a few seafarers who had inadvertently damaged the barcodes on their SIDs. The different queries can thus be summarized as shown below.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

1. Verification authority sends items 1 – 4 from Table 1 and receives “Yes“ or “No“ confirmation of validity of these items and the correct values of items 1 – 5 from Table 1 or a message that no matching SID or seafarer could be found.

2. Identical to 1 above except that the response to the enquiry also includes item 7 from Table 1, the ISO/IEC 19794-5 face image record, thus allowing for a biometric or visual check of the seafarer against both the SID photo and the record in the secure electronic database maintained by their focal point.

3. Identical to 1 above except that the response to the enquiry also includes item 6 from Table 1, the ISO/IEC 19794-2 finger minutiae record, thus allowing for a biometric check of the seafarer against the record in the secure electronic database maintained by their focal point.

4. Identical to 1 above except that the response to the enquiry also includes item 8 from Table 1, the ISO/IEC 19794-4 finger image record, thus allowing for a biometric check of the seafarer against the record in the secure electronic database maintained by their focal point. Note that the advantage of using finger images is that biometric checks may be supported by matching software that does not support ISO/IEC 19794-2 and that increased accuracy may be possible. The disadvantage is that it will require large data volumes to be transferred, possibly straining the capacity of the focal point coordination centre. Also, it is likely that many focal points may not support the optional finger image data element in their secure electronic databases or support this query.

5. Identical to 2 above except that the response to the enquiry also includes item 6 from Table 1 so that both the face and fingerprint can be verified.

6. Identical to 2 above except that the response to the enquiry also includes item 8 from Table 1 so that both the face and fingerprint can be verified.

7. Identical to 1 above except that the verification authority includes an ISO/IEC 19794-2 finger minutiae record generated from the seafarer’s primary and secondary fingers as profiled in Clause A.6.2 of this standard. The response then includes an indication of whether or not each of the primary and secondary fingers matched the corresponding fingers in item 6 for that SID in the secure electronic database managed by the focal point.

The first query in the above list shall be supported by all focal points that claim conformance to this standard and the response shall be provided to all verification authorities that have been authorized through the focal point coordination centre. All of the other queries are optionally supported and each focal point shall have the ability to decide to which, if any, ILO member states they will provide responses to queries 2 through 7. Since each verification authority shall authenticate itself securely to the focal point coordination centre server, that server shall include the information concerning the identity of the verification authority making the enquiry, including which ILO member state it is associated with and a copy of the digital certificate used to validate the verification authority, as part of each enquiry it sends to each focal point server. This is required so that the focal point servers can populate item 9 in Table 1 and so that they can decide whether or not to respond to queries 2 through 7. In cases where the focal point server does not provide a response to an enquiry, a status message shall be sent indicating whether the lack of response is due to unavailable data such as an optional data element that is not present in the secure electronic database or due to a permission issue determined by the focal point.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(normative)

Requirements list

A.1 General

Use of this Standard imposes requirements on the implementation that go beyond those of the base standards referred to by this Standard. These result in modifications to the requirements expressed in the base standards. This annex specifies the modifications (the Requirements List - RL) that apply to the status of the items affected in each Implementation Conformance Statement (ICS) proforma, with consequently modified requirements on the answers to be provided.

The meaning of the notations is as follows and in each case the base standard defines the content or behaviour of the implementation:

M Mandatory - the capability is required to be supported. In the case of values, the base standards define the content of the required element. In the case of functions, the base standard defines the required behaviour of the implementation.

N/A Not Applicable - in the given context, it is impossible to use the capability.

O Optional - the capability may be supported or not. If supported: in the case of values, the base standards define the content of the optional element; in the case of functions, the base standards define the required behaviour of the implementation.

O.i qualified optional - for mutually exclusive or selectable options from a set. “i” is an integer that identifies a unique group of related optional items and the logic of their selection, defined below the table.

X The use of this function is under the control of the application and may be subject to local agreement.

The Requirements List in this annex shall be used to restrict the permitted support answers in the corresponding ICS.

A.2 Relationship between RL and corresponding ICS proformas

In the context of the profile specification contained in this Standard, ICS proformas of the base standards contain tables in 3 categories. The 3 categories are:

- those proforma tables where this profile does not restrict the permitted support answers;
- those proforma tables where this profile restricts the permitted support answers; and
- those proforma tables that are not relevant to this profile.

The Requirements List consists of the tables falling into the second category, with an indication of the modified items in those tables.

A.3 Profile specific implementation conformance statement

The supplier of a profile implementation that is claimed to conform to this Standard shall complete the Profile specific Implementation Conformance Statement (ICS) proforma contained in this annex for those items for which implementation and conformance is claimed. All others shall be ignored.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A completed Profile specific ICS proforma is the ICS for the implementation in question. The ICS is a statement of which capabilities and options of the profile have been implemented. The ICS can have a number of uses, including use:

- by the profile implementer, as a check list to reduce the risk of failure to conform to the standard through oversight;
- by the supplier and acquirer (or potential acquirer) of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard ICS proforma;
- by the user (or potential user) of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking cannot be guaranteed, failure to interwork can often be predicted from incompatible ICS); or
- by a tester, as the basis for selecting appropriate test suites against which to assess the claim for conformance of the implementation.

A.4 Instruction for completing the ICS proforma

The following subclauses describe the procedures for completing the ICS proforma.

A.4.1 General structure of the ICS proforma

The ICS proforma is a fixed format questionnaire divided into sections each containing a group of individual items. Each item is identified by an item number, the name of the item (or section from the corresponding base standard), the operator and operand that define the possible values for the item and the reference(s) to specific clauses in the corresponding base standard. There is also a status column that indicates whether the indicated values of this item are mandatory, optional, etc. The unshaded columns on the left of the ICS proforma indicate the requirements for each item in the base standard and the shaded columns on the right of the ICS proforma indicate the requirements for each item in the profile.

Answers to the questionnaire items are to be provided in the “Support” column, by simply marking an answer to indicate a restricted choice support.

Refer to the tables below when completing this form to determine whether an item is mandatory or optional for the implementation type supplying.

A.4.2 Additional Information

Items of Additional information allow a supplier to provide further information intended to assist the interpretation of the ICS. It is not intended or expected that a large quantity will be supplied, and an ICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

A.4.3 Exception Information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirements. No pre-printed answer will be found in the Support column for this. Instead, the supplier is required to write into the support column an x.<i> reference to an item of Exception Information, and to provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to this Standard. A possible reason for the situation described above is that a defect in the standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.5 ICS proforma

Supplier	
Contact point for queries about the ICS	
Implementation Name(s)and Version(s) *	
Other information necessary for full Identification; e.g. name(s)and version(s)for machines and/or operating systems; system name(s)	
Have any exception items been required?	No [ ] Yes [ ] (The answer Yes means that the implementation does not conform to this Standard)
Date of Statement	

* *The terms "Name" and "Version" should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).*

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization © ISO/IEC 2009 – All rights reserved
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6 Interchange formats

The tables in each of the following subclauses explain the requirements of this profile when using one of the referenced base standards. The explanations of the operators and operands and how to interpret these requirements is found in the description of Level 1 and Level 2 conformance testing defined in ISO/IEC 29109-1.

A.6.1 Finger image data (ISO/IEC 19794-4)

Base Standard Requirements List						Profile Requirements List and Implementation Conformance Statement			
Item	**Section**	**Operator**	**Operands**	**Base Ref.**	**Status**	**Operator**	**Operands**	**Status**	**Support**
	General Record Header								
1	Format Identifier	EQ	0x46495200	Table 2, 8.2.2	M	EQ	0x46495200	M	
2	Version	EQ	0x30313000	Table 2, 8.2.3	M	EQ	0x30313000	M	
3	Record Length	EQ	$47 - 2^{48}$	Table 2, 8.2.4	M	EQ	$47 - 2^{48}$	M	
4	Capture Device Type ID	NONE		Table 2, 8.2.5	M	NONE		M	
5	Image Acquisition Level	EQ	10, 20, 30, 31, 35, 40, 41	Table 1& 2, 8.2.6	M	EQ	30, 31, 35, 40, 41	M	
6	Number of Finger / Palm Images	EQ	1 – 256	Table 2, 8.2.7	M	EQ	2	M	
7	Scale Units	EQ	1 – 2	Table 2, 8.2.8	M	EQ	1 – 2	M	
8	X Scan Resolution	EQ	(49-394) ppcm / (125-1000) ppi	Table 1 & 2, 8.2.9	M	EQ	(197-394) ppcm / (500-1000) ppi	M	
9	Y Scan Resolution	EQ	(49-394) ppcm / (125-1000) ppi	Table 1 & 2, 8.2.10	M	EQ	(197-394) ppcm / (500-1000) ppi	M	
10	X Image Resolution	LTE	{X Scan Resolution}	Table 2, 8.2.11	M	LTE	{X Scan Resolution}	M	
11	Y Image Resolution	LTE	{Y Scan Resolution}	Table 2, 8.2.12	M	LTE	{Y Scan Resolution}	M	
12	Pixel Depth	EQ	1 - 16	Table 1 & 2, 8.2.13	M	EQ	1 - 16	M	

13	Image Compression Algorithm	EQ	0 – 5	Table 2 & 3, 8.2.14	M	{2,4,5}	M
14	Reserved	EQ	0	Table 2, 8.2.15	M	0	M
	Finger Record Header						
15	Data Block Length	EQ	15 – 2^{32}	Table 4, 8.3.2	M	15 – 2^{32}	M
16	Finger / Palm Position	EQ	0 – 10, 13 – 15 / 20 – 36	Table 4, 5 & 6, 8.3.3	M	1 – 10	M
17	Count of Views	EQ	1 – 256	Table 4, 8.3.4	M	1 – 256	M
18	View Number	EQ	1 – 256	Table 4, 8.3.5	M	1 – 256	M
19	Finger / Palm Image Quality	EQ	-1, -2, 0 – 100	Table 4, 8.3.6	M	-1, -2, 0 – 100	M
20	Impression Type	EQ	0 – 3, 7 – 9	Table 4 & 7, 8.3.7	M	0, 1, 8, 9	M
21	Horizontal Line Length	EQ	1 – 65535	Table 4, 8.3.8	M	1 – 65535	M
22	Vertical Line Length	EQ	1 – 65535	Table 4, 8.3.9	M	1 – 65535	M
23	Reserved	EQ	0	Table 4, 8.3.10	M	0	M
	Image Data						

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization © ISO/IEC 2009 – All rights reserved
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.2 Finger minutia data (ISO/IEC 19794-2)

Base Standard Requirements List						Profile Requirements List and Implementation Conformance Statement			
Item	**Section**	**Operator**	**Operands**	**Base Ref.**	**Status**	**Operator**	**Operands**	**Status**	**Support**
	ONLY CBEFF FORMAT TYPES 3 AND 4 ARE PERMITTED								
	Record Header								
1	Format Identifier	EQ	0x464D5200	Table 7, 7.3.1	M	EQ	0x464D5200	M	
2	Version	EQ	0x20323000	Table 7, 7.3.2	M	EQ	0x20313000	M	
3	Record Length	EQ	24 – 4294967295	Table 7, 7.3.3	M	EQ	36 - 556	M	
4	Capture Equipment Certification	NONE		Table 7, 7.3.4	M	NONE		M	
5	Capture Device Type ID	NONE		Table 7, 7.3.5	M	NONE		M	
6	Image Size X	NONE		Table 7, 7.3.6	M	NONE		M	
7	Image Size Y	NONE		Table 7, 7.3.7	M	NONE		M	
8	Resolution X	GTE/EQ/EQ	98 / 1000 / 100	Table 7, 6.3.1, 7.3.8, 8.2	M	EQ	1000	M	
9	Resolution Y	GTE/EQ/EQ	98 / 1000 / 100	Table 7, 6.3.1, 7.3.9, 8.3	M	EQ	1000	M	
10	Number of Finger Views	EQ	0 – 176	Table 7, 7.3.10, 7.4.1.2	M	EQ	2	M	
11	Reserved	EQ	0	Table 7, 7.3.11	M	EQ	0	M	
	Single Fingerheader Record								
12	Finger Position	EQ	0 – 10	Table 2 & 7, 7.4.1.1	M	EQ	0 - 10	M	
13	View Number	EQ	0 – 15	Table 7, 7.4.1.2	M	EQ	0	M	

14	Impression Type	MO	{0, 1, 2, 3, 8}	Table 3 & 7, 7.4.1.3	M	{0, 1, 8}	M
15	Finger Quality	EQ	0 – 100	Table 7, 7.4.1.4	M	0 - 102	M
16	Number of Minutiae	EQ	1 – 255	Table 7, 7.4.1.5	M	0 - 52	M
	Single Finger Info						
17	Minutiae Type	EQ	0 – 2	Table 8, 8.2	M	0 - 2	M
18	Minutiae X coordinate	EQ	0 – 16383	Table 8, 8.2	M	0 – 16383	M
19	Reserved	EQ	0	Table 8, 8.2	M	0	M
20	Minutiae Y coordinate	EQ	0 – 16383	Table 8, 8.2	M	0 – 16383	M
22	Minutiae Angle	EQ	0 – 255	Table 8, 8.2	M	0 - 255	M
	Extended Data						
23	Extended Data Block Length	EQ	0	Table 7, 7.5.1.1, A.4	M	0	M

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization © ISO/IEC 2009 All rights reserved
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6.3 Face image data (ISO/IEC 19794-5)

Base Standard Requirements List						Profile Requirements List and Implementation Conformance Statement			
Item	**Section**	**Operator**	**Operands**	**Base Ref.**	**Status**	**Operator**	**Operands**	**Status**	**Support**
	Facial Header								
1	Format Identifier	EQ	0x46414300	Table 2, 5.4.1	M	EQ	0x46414300	M	
2	Version	EQ	0x30313000	Table 2, 5.4.2	M	EQ	0x30313000	M	
3	Record Length	EQ	57 - (2^{32}-1)	Table 2, 5.4.3	M	EQ	57 - (2^{32}-1)	M	
4	Number of Facial Images	EQ	1 - 65535	Table 2, 5.4.4	M	EQ	1	M	
	Facial Data								
	Facial Information								
5	Facial Record Data Length	EQ	43 - (2^{32}-15)	5.5.1	M	EQ	43 - (2^{32}-15)	M	
6	Number of Feature Points	EQ	0 - 65535	5.5.2	M	EQ	0 - 65535	M	
7	Gender	EQ	0 - 2, 255	Table 3, 5.5.3	M	EQ	0 - 2, 255	M	
8	Eye Colour	EQ	0 - 7, 255	Table 4, 5.5.4	M	EQ	0 - 7, 255	M	
9	Hair Colour	EQ	0 - 7, 255	Table 5, 5.5.5	M	EQ	0 - 7, 255	M	
10	Property Mask	EQ	0x00 - 0x7FF	Table 6, 5.5.6	M	EQ	0x00 - 0x7FF	M	
11	Expression	EQ	0 - 7, 32768 - 65535	Table 7, 5.5.7, 7.2.3	M	EQ	0 - 7	M	
12	Pose Angle Yaw	EQ	0 - 181	5.5.8.1, 7.2.2	M	MO	{0,1,2,3,179,180,181) represents -5 to 5 degrees	M	
13	Pose Angle Pitch	EQ	0 - 181	5.5.8.2, 7.2.2	M	EQ	{0,1,2,3,179,180,181) represents -5 to 5 degrees	M	
14	Pose Angle Roll	EQ	0 - 181	5.5.8.3, 7.2.2	M	EQ	{0 - 5, 177 - 181) represents -8 to 8 degrees	M	
15	Pose Angle Uncertainty Uy	EQ	0 - 181	5.5.9,	M	EQ	0 - 181	M	
16	Pose Angle Uncertainty Up	EQ	0 - 181	5.5.9	M	EQ	0 - 181	M	

17	Pose Angle Uncertainty Ur	EQ	0 - 181	5.5.9	M	EQ	0 - 181	M	
	Feature Point(s)								
18	Feature Point Type	EQ	1	Table 8, 5.6.1	M	EQ	1	O.1	
19	Feature Point Code	EQ	See NOTE 1	Table 8, Figures 6 & 7, 5.6.2	M	EQ	See NOTE 1	O.1	
20	X coordinate	EQ	0 - ({Width}-1)	Table 8	M	EQ	0 - ({Width} -- 1)	O.1	
21	Y coordinate	EQ	0 - ({Height} -1)	Table 8	M	EQ	0 - ({Height} -1)	O.1	
22	Reserved	EQ	0	Table 8	M	EQ	0	O.1	
	Image Information								
23	Face Image Type	EQ	0 - 2	Table 10, 5.7.1	M	EQ	1	M	
24	Image Data Type	MO	{0, 1}	Table 11, 5.7.2	M	MO	{0, 1}	M	
25	Width	C	See NOTE 2	5.7.3, 8.3, 8.4.1, Table 15	M	C	See NOTE 2	M	
26	Height	C	See NOTE 2	5.7.4, 8.3, 8.4.1, Table 15	M	C	See NOTE 2	M	
27	Colour Space	MO	{0 - 4, 128 – 255}	Table 12, 5.7.5, 7.4.2.3	M	MO	{1, 2, 3)	M	
28	Source Type	MO	{0 - 7, 128 – 255}	Table 13, 5.7.6	M	MO	{0 - 7, 128 – 255}	M	
29	Device Type	EQ	0 - 65535	5.7.7	M	EQ	0 - 65535	M	
30	Quality	EQ	0	5.7.8	M	EQ	0	M	
	Image Data								

NOTE 1 Each feature point code is a value consisting of A*16+B where A is the major value and B the minor value in the table below. This means that all feature point codes shall be in one of the ranges in the table.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization © ISO/IEC 2009 All rights reserved
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Major value	Minor value	Range of Valid Feature Point Codes
2	1 – 14	33 – 46
3	1 – 14	49 – 62
4	1 – 6	65 – 70
5	1 – 4	81 – 84
6	1 – 4	97 – 100
7	1	113
8	1 – 10	129 – 138
9	1 – 15	145 – 159
10	1 – 10	161 – 170
11	1 – 6	177 – 182
12	1 – 4	193 – 196

NOTE 2 The relationships between image width, image height, head width, head height and head position are described in Clauses 8.3.1 through 8.3.6 of ISO/IEC 19794-5:2005/Cor.2:2008.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

A.6.4 ISO/IEC 19785 (CBEFF)

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

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

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

Not for Resale

© ISO/IEC 2009 – All rights reserved

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

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

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(normative)

CBEFF patron format for the SID

B.1 Patron

ISO/IEC JTC 1/SC 37

B.2 Patron identifier

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

B.3 Patron format name

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

B.4 Patron format identifier

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

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

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

or, in XML value notation,

```
1.1.19785.0.257.1.9
```

B.6 Domain of use

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

B.7 Version identifier

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

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.8 CBEFF version

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

B.9 General

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

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

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

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

b) the BDB length is less than 2048 bytes.

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

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

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

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

B.10 Bit oriented patron format specification and conformance statement

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

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.10.1 Specification

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

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

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

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

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

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

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

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

      sb          SID-Security-Block }

END
```

B.11 Patron format conformance statement

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

B.11.1 Identifying information

Required Information	Patron format reference
Patron name	See B.1
Patron identifier	See B.2
Patron format name	See B.3
Patron format identifier	See B.4
Patron format ASN.1 object identifier	See B.5
Domain of use description	See B.6
Patron format version	See B.7
CBEFF version	See B.8

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.11.2 CBEFF-defined data elements and abstract values

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

B.11.3 Patron defined data elements and abstract values

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

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(normative)

CBEFF security block for the SID

C.1 Introduction

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

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

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

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

c) the digital signature (64 bytes)

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

signature = r, s

This binary signature value becomes the Signature Field.

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

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

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

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.2 SB owner

ISO/IEC JTC 1/SC 37

C.3 SB owner identifier

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

C.4 SB format name

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

C.5 SB format identifier

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

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

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

or, in XML value notation,

1.1.19785.0.257.1.3

C.7 Version identifier

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

C.8 SB specification

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

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

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

END
```

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.9 Size of the SB encoding

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

The total is 76 bytes

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

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] Federal Information Processing Standard (FIPS 180-3) “Draft Secure Hash Standard” (draft)

[2] Federal Information Processing Standard (FIPS 186-3) “Draft Digital Signature Standard” (draft)

[3] ILO Convention No. 185 - Seafarers' Identity Documents Convention (Revised), 2003

[4] ILO SID-0002 – Convention No. 185 – Seafarers' Identity Documents Convention (Revised), 2003 – The standard for the biometric template required by the Convention, Second impression (with modifications), 2005, ISBN 92-2-115788-1

[5] ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*

[6] ISO/IEC TR 14516:2002, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[7] ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

[8] X9.62-2005, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA)”

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 37 pages

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale