

---

---

**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*

get full document from [standards.iteh.ai](https://standards.iteh.ai)

**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.

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from 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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	v
Introduction.....	vi
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

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**

get full document from [standards.iteh.ai](https://standards.iteh.ai)

## 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*

## 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.

# 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 24713-3:2009(E)

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 bibliography 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 enrollee

### 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)

**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****enrollee**

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

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;

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.

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.