TMCASI/C.185/2016(Rev.)

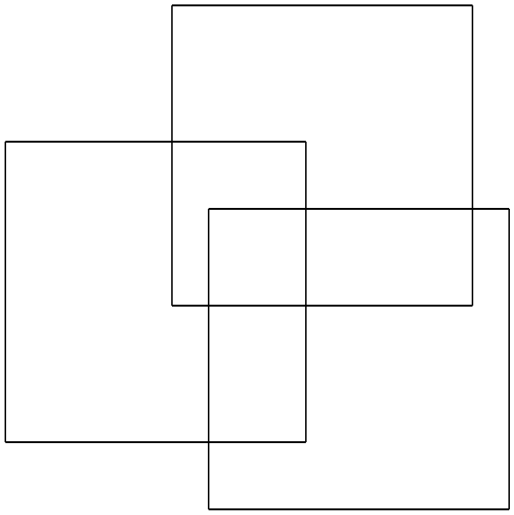
International
Labour
Office

Geneva

Background paper for the meeting of the Ad Hoc Tripartite Maritime Committee established for the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)

(Geneva, 10–12 February 2016)

Commentary and draft proposals for amendments to Annex I, Annex II and Annex III of Convention No. 185



Geneva, 2016

International
Labour
Standards
Department

TMCASI/C.185/2016(Rev.)

INTERNATIONAL LABOUR ORGANIZATION

International Labour Standards Department

Background paper for the meeting of the Ad Hoc Tripartite Maritime Committee established for the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)

(Geneva, 10–12 February 2016)

Commentary and draft proposals for amendments to Annex I, Annex II and Annex III of Convention No. 185

Geneva, 2016

INTERNATIONAL LABOUR OFFICE

First edition 2016

Background paper for the meeting of the Ad Hoc Tripartite Maritime Committee established for the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), Geneva, 10–12 February 2016, International Labour Office, International Labour Standards Department, Geneva, ILO, 2015.

ISBN 978-92-2-130270-4 (print)
ISBN 978-92-2-130271-1 (Web pdf)

Also available in French: *Document de travail pour la réunion de la Commission tripartite maritime ad hoc chargée de l'amendement de la convention (no 185) sur les pièces d'identité des gens de mer (révisée), 2003*, Genève, 10-12 février 2016, ISBN 978-92-2-230270-3 (print), 978-92-2-230271-0 (Web pdf), Geneva, 2016; and in Spanish: *Documento de referencia para la reunión del Comité Tripartito Marítimo ad hoc para la enmienda del Convenio sobre los documentos de identidad de la gente de mar (revisado), 2003 (núm. 185)*, Ginebra, 10-12 de febrero de 2016, ISBN 978-92-2-330270-2 (print), 978-92-2-330271-9 (Web pdf), Geneva, 2016.

Printed by the International Labour Office, Geneva, Switzerland

Contents

Appendix

List of abbreviations

CPO	central processing office
CSCA	Country Signing Certification Authority
ICAO	International Civil Aviation Organization
ILO	International Labour Organization
ISO	International Organization for Standardization
LDS	Logical Data Structure
MRZ	machine-readable zone
PKD	Public Key Directory
PKI	Public Key Infrastructure
SID	seafarers' identity document
TD1	Size 1 machine-readable official travel document
TD3	Size 3 machine-readable official travel document
VIZ	visual-inspection zone

Introduction

1. In February 2015, a tripartite Meeting of Experts concerning the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), was convened to consider difficulties that had arisen with respect to the implementation of that Convention – particularly in connection with the biometric (based on fingerprint technology) that the Convention requires to be placed on the seafarers' identity document (SID). [1] A clear majority of experts at this three-day meeting concluded that the most feasible way forward was for the International Labour Conference to amend Annex I to the Convention and, as necessary, the other Annexes to it, in order to align the biometric under Convention No. 185 with the standards of the International Civil Aviation Organization (ICAO), which were now universally followed for travel and similar documents.

2. The Meeting accordingly requested the Governing Body of the International Labour Office to convene a meeting in 2016 of the "duly constituted tripartite maritime body" referred to in Article 8, paragraph 1, of the Convention, to advise the International Labour Conference on the adoption of amendments to the Annexes to the Convention, and made the following recommendation: [2]

> Recommendation 1: The International Labour Office should prepare a preliminary draft of a revised Annex I and Annex II of Convention No. 185 where the biometric is changed from a fingerprint template in a two-dimensional barcode to a facial image stored in a contactless chip and where the national electronic database is required to contain only the public keys required to verify the digital signatures defined for the contactless chip by ICAO Document 9303. All references to technical standards other than ICAO Document 9303 are to be eliminated, as all of the ISO standards required would now already be referenced within ICAO Document 9303. The references to ICAO Document 9303 should refer to that document, including subsequent amendments of it, so that the Annexes will not require changing in the future as ICAO issues new versions of ICAO Document 9303 and as ePassport technology moves forward. If any of the changes to Annex I and Annex II need to be reflected in changes to the processes and procedures outlined in Annex III (such as, for instance, a need to ensure the quality of the photograph of the seafarer), then these changes may have to be reflected in a preliminary draft of a revised Annex III.

3. At its 323rd Session (March 2015), the Governing Body took note of the general conclusion and the recommendations of the tripartite Meeting of Experts and decided to convene an Ad Hoc Tripartite Maritime Committee to make proposals, based on the recommendations of the Meeting of Experts, for consideration by the International Labour Conference at its 105th Session (2016), under an agenda item entitled "Amendment of the Annexes to the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)".[3]

[1] Information about the Meeting, including background papers and the report on the discussions, is available on the ILO's Maritime Labour Convention, 2006, web page at: http://www.ilo.org/global/standards/maritime-labour-convention/events/WCMS_301223/lang--en/index.htm.

[2] ILO: *Outcome of the Meeting of Experts concerning the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185) (Geneva, 4–6 February 2015)*, Governing Body, 323rd Session, Geneva, Mar. 2015, GB.323/LILS/4. The general conclusion and recommendations of the Meeting of Experts are contained in the appendix to that document.

[3] ILO: *Minutes of the 323rd Session of the Governing Body of the International Labour Office*, Governing Body, 323rd Session, Geneva, Mar. 2015, GB.323/PV, para. 360.

4. To assist the Ad Hoc Tripartite Maritime Committee, and as recommended by the Meeting of Experts in February 2015, the Office has prepared a preliminary draft proposal (hereinafter referred to as "the preliminary draft") for the amendment of Annexes I and II to Convention No. 185 (and for the consequential adjustment of Annex III) with all the changes from the current version of the Annexes clearly marked. The preliminary draft is contained in Part I of this background paper. Part II of this background paper explains the main changes that would need to be made by governments in the implementation of Convention No. 185, especially in connection with the system for issuing SIDs, if the amendments proposed in the preliminary draft were adopted by the International Labour Conference in June 2016.

5. The Ad Hoc Tripartite Maritime Committee is accordingly invited to propose to the International Labour Conference amendments to the Annexes to Convention No. 185, based on the preliminary draft in Part I below, and taking account of the explanations in Part II.

6. Another recommendation of the tripartite Meeting of Experts noted by the Governing Body concerned the date of entry into force of the amendments to the Annexes and transitional arrangements. This recommendation, which was based mainly on Article 3, paragraph 1, of the Convention, [4] stated as follows:

> Recommendation 6: Due to the importance of supporting the existing SID system as these changes in technology are implemented, there should be a suitable transitional period**.**
>
> *Entry into force and transitional period*
>
> *Entry into force*
>
> 1. The amendments will enter into force one year after their adoption by the International Labour Conference in accordance with paragraph 1 of Article 8 of the Convention.
>
> *Transitional period*
>
> 2. Members whose ratification of the Convention was registered prior to the date of entry into force referred to in paragraph 1 above may, for a further period not exceeding three years after entry into force, continue to issue SIDs in accordance with the Convention prior to the amendment of its Annexes.
>
> *Saving provision*
>
> 3. The entry into force of the amendments or the expiry of the previous transitional period will not affect any SIDs issued under the prior provisions that were still in force at that time. They will continue in force until their expiry date or until the date for the SIDs renewal in accordance with Article 3, paragraph 6, of the Convention, if that date is earlier.

7. The Ad Hoc Tripartite Maritime Committee may wish to confirm its agreement with recommendation 6 concerning the proposed time frame for the entry into force of the proposed amendments and the proposed transitional arrangements.

8. Part III of this background paper sets out various options as to how ratifying Members might implement a cost-effective SID-issuance system under the amended Annexes. Although the Ad Hoc Tripartite Maritime Committee is not called on to make a decision in this regard, as such matters are for each Member to decide, before proposing amendments to the International Labour Conference, the Committee would need to be satisfied that such amendments would, in practice, enable ratifying Members to fully implement Convention No. 185.

[4] See also Article 4, paragraph 2, and Article 5, paragraph 3, of the Convention.

I. Preliminary draft for amendments to the Annexes

9. Annex I to the Convention, entitled "Model for seafarers' identity document", would be entirely replaced by the text set out below. The editorial footnotes are for information only and would not be part of the final text of the Annex.

Annex I

Model for seafarers' identity document

Subject to the overriding requirements of Article 3 of this Convention, the seafarers' identity document (SID), whose form and content are set out below, shall – with respect to the materials used for it and the presentation and storage of the data that it contains – conform to the mandatory requirements for a TD1-size electronic machine-readable official travel document contained in International Civil Aviation Organization (ICAO) Document 9303 on machine-readable travel documents, with full consideration being given to any relevant recommendations or advice in that document. The term "Document 9303" shall be understood as referring to the Seventh Edition, 2015, as published by ICAO and as it may subsequently be amended in accordance with the related procedures of ICAO. References in this Annex to particular provisions of Document 9303 refer to the Seventh Edition, but shall be understood as also referring to the corresponding provisions of any subsequent edition. The Director-General of the International Labour Office may from time to time, as requested by the Governing Body, prepare guidance for Members as to the specific provisions of Document 9303 to be taken into account.

The SID shall be an electronic machine-readable identity document of TD1-size with physical characteristics as described in Section 2 of Part 3 of Document 9303, "Specifications Common to all Machine Readable Travel Documents". The printing and typefaces used in both the visual-inspection zone and the machine-readable zone shall be as described in Sections 3 and 4 respectively of Part 3 of Document 9303. The size of the identity document shall be as specified in Section 2 of Part 5 of Document 9303, "Specifications for TD1 Size Machine Readable Official Travel Documents" and the layout of all the data elements shall be as specified in Section 3 of Part 5.

The SID shall include a contactless integrated circuit, with a data storage capacity of at least 32 kilobytes, encoded and digitally signed in accordance with Parts 9, 10, 11 and 12 of Document 9303. The contactless integrated circuit shall meet all the requirements for the Logical Data Structure (LDS) set out in Part 10 of Document 9303 but shall contain only the mandatory data elements required in that Part. The privacy of seafarers' data stored in the contactless integrated circuit shall be protected by a Chip Access Control mechanism as described in Part 11 of Document 9303. Data stored in the LDS shall be limited to the metadata and files required for the operation of the chip and its security features, as well as the following data elements, which are already visible, in the sense of eye-readable, in the visual-inspection and machine-readable zones of the SID:

(i) in data group 1 of the LDS: a duplication of the machine-readable zone data, referred to below;

(ii) in data group 2 of the LDS: the biometric representation required by Article 3, paragraph 8, of this Convention, which shall comply with Part 9 of Document 9303 for the "Primary Biometric: Facial Image". This facial image of the seafarer shall be a copy of the photograph referred to in (o) below, but compressed to a size in the range of 15–20 kilobytes;

(iii) the Document Security Object that is needed to validate the integrity of data stored in the LDS using the ICAO Public Key Infrastructure defined in Part 12 of Document 9303.

The SID shall be protected from tampering, photograph substitution or other fraudulent activity by adherence to the requirements of Part 2 of Document 9303, "Specifications for the Security of the Design, Manufacture and Issuance of MRTDs". It shall be protected by at least three physical security features from the list contained in Appendix A to Part 2 of Document 9303. Examples of such security features include:

- optically variable features [5] in the substrate or laminate of the identity document;
- tactile features [6] in the substrate of the identity document;
- laser-perforated features [7] in the substrate;
- two-colour guilloche design [8] in the background of the identity document;
- microprinted text [9] in the background;
- ultraviolet fluorescent ink;
- ink with optically variable properties;
- steganographic image [10] incorporated in the identity document.

The data elements to be contained in the identity document and their placement within the various zones described in Part 5 of Document 9303 are given below and no other information shall be contained in the SID:

(a) issuing State: name in full, in Zone I, with no field caption;

(b) document type: "SID", in Zone I, with no field caption;

(c) "chip inside" symbol described in Section 2.3 of Part 9 of Document 9303: in Zone I, with no field caption;

(d) full name of seafarer as a single field consisting of the primary identifier followed by a comma, then a space and then the secondary identifier, as defined in Part 5 of Document 9303: in Zone II, with a field caption;

(e) sex of seafarer as a single letter, "F" for female, "M" for male or "X" for unspecified: in Zone II, with a field caption;

(f) nationality of seafarer, as a three-letter International Organization for Standardization country code: in Zone II, with a field caption;

(g) date of seafarer's birth, in the format DDbMMbYYYY, where "b" is a single blank space (for example, 23 03 1982): in Zone II, with a field caption;

(h) place of seafarer's birth: in Zone II, with a field caption;

(i) any special physical characteristics that may assist in the identification of the seafarer: in Zone II, with a field caption. If the issuing authority chooses not to record any identifying characteristics or if the seafarer has no particular identifying characteristics then this field shall be filled with the English word "None";

(j) unique document number assigned to the SID by the issuing authority, of no more than nine characters: in Zone III, with a field caption;

[5] Editor's note: An optically variable feature is an image or feature whose appearance in colour or design changes depending on the angle of viewing or illumination.

[6] Editor's note: A tactile feature is a surface feature giving a distinctive "feel" to the document.

[7] Editor's note: Laser perforation is a process whereby numbers, letters or images are created by perforating the substrate with a laser.

[8] Editor's note: A guilloche design is a pattern of continuous fine lines, usually computer generated, forming a unique image that can only be accurately re-originated by access to the equipment, software and parameters used in creating the original design.

[9] Editor's note: Microprint is printed text or symbols smaller than 0.25 mm/0.7 pica points.

[10] Editor's note: Steganography is the use of an image or information that is encoded or concealed within a primary visual image.

(k) date of issue of the SID, in the format DDbMMbYYYY, where "b" is a single blank space (for example, 31 05 2014): in Zone III, with a field caption;

(l) date of expiry of the SID, in the format DDbMMbYYYY, where "b" is a single blank space (for example, 31 05 2019): in Zone III, with a field caption;

(m) place of issue of the SID: in Zone III, with a field caption;

(n) signature or usual mark of the seafarer: in Zone IV, without a field caption;

(o) photograph of the seafarer, conforming to the specifications for photographs set out in Part 3 of Document 9303: in Zone V, without a field caption;

(p) the following statement in English, in Zone VI, on the back of the identity document, without a field caption:

"This document is a seafarers' identity document for the purpose of the Seafarers' Identity Documents Convention (Revised), 2003, of the International Labour Organization. This document is a stand-alone document and not a passport.";

(q) name of the issuing authority, and contact details (telephone number including country code or URL of website or both) of the focal point under Article 4, paragraph 4, of this Convention: in Zone VI, on the back of the identity document, with the following field caption in English: "Issuing authority contact details";

(r) three-line machine-readable zone printed in Zone VII as specified in Section 4 of Part 3 and Section 4.2 of Part 5 of Document 9303, containing all the mandatory data elements specified in Section 4.2 of Part 5 and using "IS" as the first two characters of the upper machine-readable line ("I" indicating that it is an identity document and "S" indicating that it is a seafarers' identity document).

10. The text below indicates the changes proposed for Annex II to the Convention.

Annex II

Electronic database

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

Section 1

1. Issuing ~~authority named on~~ State as written in the visual-inspection zone of the seafarers' identity document (SID).

2. Full name of seafarer as written ~~on the identity document~~ in the visual-inspection zone of the SID.

3. Unique nine-character document number ~~of the identity document~~ assigned to the SID.

4. Date of expiry or suspension or withdrawal of the ~~identity document~~ SID, written in the format DDbMMbYYYY, where "b" is a single blank space (for example, 31 05 2019).

Section 2

5. ~~Biometric template appearing on the identity document.~~Compressed facial image of the seafarer as stored in the contactless integrated circuit of the SID.

6. Photograph of the seafarer as printed in the visual-inspection zone of the SID.

7. Details of all inquiries made concerning the ~~seafarers' identity document~~ SID.

11. The addition of the underlined paragraph below is proposed for Annex III to the Convention.

Annex III

Requirements and recommended procedures and practices concerning the issuance of seafarers' identity documents

This Annex sets out minimum requirements relating to procedures to be adopted by each Member in accordance with Article 5 of this Convention, with respect to the issuance of seafarers' identity documents (referred to below as "SIDs"), including quality-control procedures.

Part A lists the mandatory results that must be achieved, as a minimum, by each Member, in implementing a system of issuance of SIDs.

Part B recommends procedures and practices for achieving those results. Part B is to be given full consideration by Members, but is not mandatory.

Notwithstanding the above, in implementing Part A, each Member shall observe all relevant mandatory requirements in International Civil Aviation Organization (ICAO) Document 9303. The term "Document 9303" shall be understood as referring to the Seventh Edition, 2015, as published by ICAO and as it may subsequently be amended in accordance with the related procedures of ICAO. In addition to giving full consideration to Part B of this Annex, Members shall give full consideration to the relevant recommendations or advice contained in Document 9303, especially in Part 2 of that document and its appendices.

Part A. Mandatory results

[No change is proposed for Part A of Annex III.]

Part B. Recommended procedures and practices

[No change is proposed for Part B of Annex III.]

II. Main changes to the SID and to the issuance process arising from proposed changes

A. Physical layout and card material

12. Annex I of Convention No. 185 currently allows a SID to be either the size of a credit card (TD1) or of a single page from a passport book (TD3). The TD3 size allows more space to include information on the SID, but is less convenient for the seafarer as it cannot fit easily in a wallet or other form of credit card holder.

13. The preliminary draft in Part I proposes that only the TD1-size document should be permitted. This is because the SID would have to be made of a substrate which can hold a contactless chip and antenna, and a single page document of passport size (TD3) can be bent more easily and may reduce the lifetime of the chip. The preliminary draft also proposes the removal of the two-dimensional bar code, which would leave more space available on the back of the TD1-size SID. This means that a larger (TD3) size document to fit in all the necessary data elements with translations is no longer needed.

14. The preliminary draft refers to the seven zones indicated in Document 9303, namely:

- Zone I: Mandatory header
- Zone II: Mandatory and optional personal data elements
- Zone III: Mandatory and optional document data elements
- Zone IV: Mandatory holder's signature or usual mark
- Zone V: Mandatory identification feature
- Zone VI: Optional data elements (back of the card)
- Zone VII: Mandatory machine-readable zone (MRZ) (back of the card)

Zones I–VI form the visual-inspection zone (VIZ).

15. The SID would need to be made from a physical substrate which is resilient enough to protect the contactless chip in normal use. PVC or polycarbonate are excellent choices for the material of the card, but laminated paper SIDs are no longer possible as they would not provide sufficient stiffness and the chip antenna would easily break. According to the proposals in the preliminary draft, the positioning of the data elements (name, date of birth, and so on) printed on the SID would be virtually identical to the positioning under the current version of Annex I to the Convention. Although the main data elements themselves would also be very similar, a few changes have been proposed in the preliminary draft to ensure that the presentation of the data elements would be fully consistent with that described in the latest edition of Document 9303. [11] It would, therefore, be important for all issuers to ensure that the presentation of each data element and the field caption (or absence of caption) is exactly as described in the list provided in the revised version of

[11] The text of all parts of Document 9303, Seventh Edition, 2015, are available for download at http://www.icao.int/publications/pages/publication.aspx?docnum=9303.

Annex I. A sample of a SID that reflects these elements is set out in the appendix to this paper.

16. All SIDs need to have sufficient security features to ensure that they are resistant to fraud. While digital security features are already part of the chip, the SID also needs to have physical security features in case the entity verifying the identity of the seafarer does not have access to ePassport readers, which are connected to the necessary Public Key Infrastructure (PKI), to verify the digital security. The present version of Annex I requires only one security feature from a fairly limited list. According to the preliminary draft, the revised version of Annex I would require a minimum of three security features from Appendix A to Part 2 of Document 9303. Many identity documents will use more than three physical security features and the supplier of the documents will be able to advise on all the security features of a particular document, but it is important to ensure that at least three of these physical security features are in the list from Appendix A to Part 2 of Document 9303.

B. Biometric features and biometric enrolment

17. One of the most important differences as compared with the present wording of the Annexes to Convention No. 185 is that the "template or other representation of a biometric of the holder" which is required by Article 3, paragraph 8, of the Convention, would be changed from a fingerprint printed as numbers in a bar code to a "Primary Biometric: Facial Image" as defined in Part 9 of Document 9303. This would have a significant impact on the implementation of Convention No. 185, both in terms of the issuance of SIDs and on their verification at ports and border crossings.

18. First, this change would overcome the challenge of achieving interoperability, that is, of ensuring that the biometric in a SID issued in any ratifying country will be verifiable in all other countries. Since the biometric verification of a seafarer would now be conducted using facial recognition rather than fingerprint recognition, there would no longer be a need for the ILO to ensure interoperability by creating a list of biometric products that it has tested and found to meet the requirements of the Convention. The "Primary Biometric: Facial Image" defined in Document 9303 is a compressed and formatted representation of the seafarer's own face. All known facial recognition products are able to work with images of this type and any interoperability issues are already being addressed by the ICAO and the global community of passport-issuance authorities and border authorities.

19. A second change is that it would no longer be necessary to see a seafarer in person whenever a SID is being issued in order to capture the seafarer's fingerprints. This would allow for the possibility of a SID being issued through a postal or other secure system without a seafarer needing to come into an office. Obviously this would not be appropriate for the initial issuance of a SID, when the seafarer needs to be seen by an official to ensure that they are a legitimate seafarer and to verify that the photograph being used for their biometric data is a photograph of the right person. For renewals, however, the seafarer could simply send in an application form, their old SID and a new photograph. The photograph could then be checked against the old SID and the image of the seafarer maintained in the national electronic database to verify that it is a legitimate representation of the same seafarer. After that, the new SID could be issued and mailed to the seafarer. This would be optional and individual issuing authorities could still choose to require a personal visit by the seafarer for both initial issuance and subsequent renewal.

20. As the issuance process would no longer require fingerprint capture, there would be no need to use any fingerprint hardware or software in the issuance process. The facial image can be acquired either by taking a photograph of the seafarer or by scanning a printed photograph. More importantly, the verification process would no longer require any

fingerprint hardware or software and could be completed using the same infrastructure that is already available at border crossing points for verifying the identity of holders of ePassports.

21. The introduction of the facial image as the biometric of the holder of the SID would require issuing authorities to place more importance on acquiring a high-quality facial image than was previously necessary. Recent evidence provided to the International Organization for Standardization (ISO) from automated border control systems in Australia and New Zealand shows that the performance of the facial recognition algorithms used in the border control systems varies significantly, depending on the country which issued the ePassport held by the traveller. For the most part, this performance difference seems to be related to the quality of the ePassport image. Although the ISO is still developing new recommendations based on this evidence, the following issues have been identified and all SID-issuing authorities should pay careful attention to them when taking photographs of seafarers or when deciding to accept or reject photographs submitted by seafarers for use with their SIDs:

(a) It is vital to follow the guidelines on facial expression, lighting and head coverings described in Section 3.9 of Part 3 of Document 9303. If a live-captured image or a submitted photograph does not follow these guidelines, then it must be rejected and another image or photograph acquired.

(b) Although not required by Document 9303, it is strongly recommended that photographs be taken without the seafarer wearing corrective or reading glasses, even if they are usually worn.

(c) When cropping a photograph or scanning it from a printed image, it is important to ensure that no lines appear in the cropped photograph due to different background colours (such as between the scanner background and the background of the photograph). Any distinct vertical or horizontal lines in the background will have a negative impact on the quality of the image once it is compressed for storage in the contactless chip.

(d) Compression should take place only once, so original scanned images should be stored at full scanner resolution and then compressed for storage in the contactless chip.

(e) Quality-control procedures should always involve a step to view the image stored in the chip to ensure that it is of sufficient quality and to ensure that it matches the image printed on the SID.

C. Encoding the chip

22. Under the preliminary draft, Annex I would no longer require a two-dimensional bar code. Instead, seafarer data, including the biometric information, would be stored in a contactless chip. This means that, if the Annexes are revised as envisaged, all SID-issuing authorities would need to add a new step in the issuance process, in which the necessary data would need to be encoded into the Logical Data Structure (LDS) contained in the contactless chip. This would be part of the personalization process, in which a blank document is turned into a finished SID, containing the personal details of an individual seafarer.

23. The addition of card encoding in the personalization process means that it would now be vitally important to ensure that the data printed on the SID and the data contained within the contactless chip match. Ideally, the encoding of the chip and the printing of the SID would take place in a single step, using a printer which is also capable of encoding the

contactless chip. If this is not possible, it would be critical to ensure that the issuance software properly tracks each document as it passes from the print stage to the separate encoding stage or vice versa. In either case, there would need to be a new quality assurance step in the issuance process, in which the data from the contactless chip and the data printed on the card (both in the visual-inspection zone (VIZ) and in the machine-readable zone (MRZ)) would be reviewed to ensure that all three sets of the personal details of the seafarer (in the VIZ, the MRZ and in the chip) and both photographs (the one printed in the VIZ and the one stored in the chip) are the same.

24. The use of the contactless chip also means that new machines would need to be made available to satisfy Article 3, paragraph 9, of Convention No. 185, which states, among other things, that "Seafarers shall have convenient access to machines enabling them to inspect any data concerning them that is not eye-readable". In practice, this would require the issuing authority to provide a system which could read the data from the chip and display it on a screen so that the seafarer could inspect it. The same system used for the quality-assurance step mentioned in the previous paragraph could be used, as it would not only display the information from the chip but would also display the corresponding information from the MRZ and the VIZ so that seafarers could easily verify that all their personal data are accurate.

25. It is important to note that the addition of the contactless chip and the equipment to encode it and read it would add cost to the SID-issuance system and to each SID produced. The corresponding advantage, however, would be that the infrastructure to read and decode information from contactless chips encoded in accordance with Document 9303 already exists at many border crossings, whereas the infrastructure to read and decode two-dimensional bar codes is virtually non-existent.

26. Since the contactless chip and its antenna are hidden inside the body of the card being personalized into a finished SID, issuing authorities would need to acquire blank SIDs containing suitable contactless chips and would be unable to use any previous card stock that they might have acquired for use with the current versions of the Annexes to Convention No. 185. Also, it would be important to ensure that the contactless chips used in SIDs were fully compatible with the requirements in Document 9303, especially Parts 10, 11 and 12. This would most easily be accomplished by procuring a chip which had already been used in a previous ePassport issuance system.

27. The specific details of the structure of the Data Groups in the LDS for a contactless chip are specified in Part 10 of Document 9303, and since the proposed revised Annexes to Convention No. 185 would only use Data Groups 1 and 2, together with the Document Security Object (EF.SOD), this is a fairly simple structure. The contactless chip, however, would still need to meet all the ISO standards for proximity contactless integrated circuit-based electronic machine-readable travel documents which are listed in Part 10 of Document 9303, and this means that encoding the Data Groups into a simple read-only chip would not be sufficient. The contactless chip would need to support the necessary access methods and security protocols and so it would need to be a chip that had been tested for use in ePassports.

28. The methods used to protect the data on the contactless chip and to ensure that the data have been written by a legitimate issuing authority are also quite complex and this means that SID-issuing authorities would need to use chips that had been tested for use in ePassports, and also software for digital signing and for the generation of cryptographic certificates that had been tested for use with ePassports. The details of the security mechanisms and the cryptographic systems are provided in Parts 11 and 12 of Document 9303 and these are probably the most technically complex part of the process of issuing a SID in full compliance with Document 9303. The use of the Public Key Infrastructure

(PKI), in particular, would require some effort from issuing authorities and is discussed in more detail below.

D. Public Key Infrastructure

29. In order to discuss the PKI required by Document 9303, it is first necessary to understand in general how digital signatures work.

30. The first important concept is a cryptographic key pair. Using complex mathematics which depend on the specific cryptographic algorithm being used, two linked keys are generated. Each key is simply a large random number used as a parameter in a specific cryptographic algorithm, but together they share the property that what is encrypted with one key can only be decrypted with the other, and vice versa. One key is called the private key and is intended to be kept as a very secure secret by the owner of the keys, and the other is called the public key and can be distributed freely to everyone. If the owner of the keys encrypts a string of data, such as the words "Seafarer identity document" with the private key, then it will become a random string of gibberish that cannot be linked back to the original meaning. Anyone who has a copy of the public key, however, can decrypt the string and see what it originally said. If they use the public key belonging to someone else, however, the decryption will fail and the string will remain as gibberish.

31. The second important concept is a "hash". A large sequence of data, such as the entire contents of the machine-readable zone of an ePassport or SID, can be run through a "hash algorithm" to produce a short string called a "hash digest". The property of the digest is that it is not possible to determine from the hash what the original data were, but any change to the original data will significantly change the hash. A simple example would be to take all the characters in the string and convert them to their values using the American Standard Code for Information Exchange (ASCII) (numbers between 0 and 255) and then add them up, divide by 100 and find the remainder. This would always result in a number between 0 and 99, no matter how long the original string. It would be impossible to calculate the original string from a single number between 0 and 99, but if even a single letter in the original string was changed, the hash digest would also change. It is clear that the actual hash algorithms used in practice are much more complex, but the principle is the same. While it is not possible for someone to compute the original string from the hash digest, where one has the original string it is possible to regenerate the hash digest.

32. By combining these two concepts, a digital signature can be created. In the case of an ePassport or SID, the authority issuing the document generates a hash of the data it wants to sign (the contents of each Data Group of the LDS of the contactless chip). It then encrypts this hash digest using its private key and stores the encrypted hash digest in the document (in the Document Security Object (EF.SOD) in the contactless chip). The border or other authority verifying the authenticity of that document will then read the contents of each Data Group from the LDS and then the corresponding encrypted hash digest from the Document Security Object. Next, it will generate its own version of the hash from the data that it has just read. Finally, the verifying authority will use the public key which corresponds to the issuing authority for the document to decrypt the encrypted hash digest. If the decrypted hash digest and the hash digest that the verifying authority generated for itself are identical, then it proves two things:

(a) that the data just read and used to generate a hash digest have not been tampered with and are exactly the same as the data that were originally used to generate the encrypted hash digest by the issuing authority; and

(b) that the authority that issued the document is the same issuing authority as the one that sent the public key to the border authority.

33. The benefit of this system is that no one can digitally sign a fraudulent or false document unless they have access to a legitimate private key whose public key has been distributed to all the verifying authorities. Also, once a document has been issued and digitally signed, it cannot be altered without changing the hash digest, which will be easily spotted when the digital signature is verified. This leads to the two most critical points in issuing a document secured by digital signatures:

(a) the private key of the issuing authority must be kept secure and can never be disclosed to any other entity;

(b) there must be a secure method for the issuing authority to provide its public key to every verifying authority in the world so that those verifying authorities know they can trust this public key as coming from a legitimate issuing authority. This is what is known as a Public Key Infrastructure, or PKI.

34. It should be noted that the situation is more complex than this basic explanation. Each key is stored in a standardized form in a certificate and the certificates are exchanged rather than the keys. There are also multiple layers of cryptographic keys so that the private key used for signing documents as they are issued is always a temporary key which is changed periodically. The trust in these temporary keys is established through their certificates being digitally signed using a single master key, which in the ICAO PKI, described in Part 12 of Document 9303, is assigned to the Country Signing Certification Authority (CSCA). The private key of the CSCA is to be very well protected and it is only used to generate new certificates when temporary keys (document signer keys) are changed. A mechanism exists to revoke certificates if a document signer key is compromised, but the CSCA key is supposed to be handled with such security that it can never be compromised. If it is, then all trust in documents issued by that country would be lost. Typically, CSCA keys are changed every three–five years, whereas document signer keys are changed every one–three months.

35. The ICAO manages a contract with a private company which runs the ICAO Public Key Directory (PKD). This is a system which allows the public keys used for ePassports to be distributed globally so that all border agencies and indeed any entity which may need to verify an ePassport can download a complete copy of the PKD. In order to gain initial access to the PKD, the issuing authority is required to arrange for one of its officials to go in person to the PKD operations centre, where the initial CSCA certificate is handed over and verified so that it can be securely entered into the PKD. This is where the trust is established. After that, there are electronic mechanisms for distributing all the secondary certificates, revocation lists and even for changing the CSCA certificate, since all these operations can be verified using the initial CSCA certificate.

36. If the Annexes to Convention No. 185 are revised as envisaged, then any Convention No. 185 authority seeking to issue SIDs in conformity with the revised Annexes would need to include a mechanism to digitally sign the contents of the LDS in the contactless chip that is fully compatible with the PKI described in Part 12 of Document 9303. This means that the public keys would need to be distributed to all border authorities and made available to other entities that might wish to authenticate SIDs. At the same time, the private keys would need to be kept extremely secure so that the trust in the certificates used to sign the SID is equivalent to the trust in certificates used to sign ePassports.

37. While it would be theoretically possible for a SID-issuing authority to set up its own Public Key Infrastructure to meet the above requirements, the practical difficulties that have been experienced in convincing border authorities to use the PKD suggest that convincing them to use a second equivalent mechanism just for SIDs would be most unlikely to succeed as the relative number of SIDs to ePassports seen by any national border authority is

extremely small. Therefore, the only practical solution would be to use the PKD as the PKI for SIDs issued under the proposed revised Annexes of Convention No. 185.

38. Becoming a full participant in the PKD is quite expensive with the fees for 2015 set at US$56,000 as the initial fee to become a participant and $43,642 as the annual fee to participate.

39. There is also a potential for confusion if the ePassport-issuing authority and the SID-issuing authority in the same country both have their own CSCA. Although this is theoretically possible within the PKD, as there are a few countries which have more than one ePassport-issuing authority, it is not the usual method for operating the PKD.

40. If a SID-issuing authority is not a PKD participant, however, it may still be able to ensure that its certificates are part of the PKD. If another entity that is part of the PKD agrees to digitally sign the CSCA certificate of the SID-issuing authority and to include it in its Master List, then it would still become part of the PKI.

41. In conclusion, there are many mechanisms that could potentially be used by a SID-issuing authority to implement the PKI requirements of Document 9303. The specific solution selected may be different for different ILO Members that ratify Convention No. 185. It may be simpler, however, if a single solution was recommended for all Members. Guidance from the ICAO would be useful in this regard, and the ICAO will be requested to provide its guidance at the meeting of the Ad Hoc Tripartite Maritime Committee when the preliminary draft in Part I of this paper is reviewed.

III. How an issuance system under the amended Annexes could be managed

42. The explanations above concerning the major changes to the SID and the SID-issuance process show that there would clearly be additional complexity and cost involved in implementing the Annexes, if revised as proposed in the preliminary draft. Under the Annexes as currently worded, all issuing authorities under Convention No. 185 use the same basic process. The current process can be broken down into the following steps:

(a) The personal details of the applicant for a SID, as well as the applicant's photograph and fingerprints, are obtained and recorded.

(b) The applicant's documents are inspected to verify the applicant's identity, citizenship or place of residence and authenticity as a seafarer.

(c) All the information about the applicant and the application for a SID is recorded and passed to a different official of the issuing authority from the one who received the application and recorded the data. This official then has to verify the application and authorize production of the SID.

(d) Various security checks take place. This may include checks with local police databases or with maritime schools or shipping companies to verify that the applicant is actually a seafarer. The specific checks performed vary.

(e) Once the security checks are passed and authorization is received, the SID is printed. This includes printing of the two-dimensional bar code in which the fingerprints are stored.

(f) The printed SID is checked to ensure that the data are correct and that all elements have been printed correctly and are readable. This step is known as quality assurance and although it is recommended that such a step be performed on every SID, it may be performed only on a subset of SIDs. A failure here means that steps (e) and (f) need to be repeated.

(g) An entry is created in the national electronic database for the SID that was just printed.

(h) The SID is issued to the seafarer.

43. All the steps listed above may be performed at the same physical location, but it is also possible to have several enrolment sites where steps (a), (b) and possibly (h) take place, with the other steps taking place at a central site.

44. If the Annexes to Convention No. 185 are revised as proposed in the preliminary draft, the new process will be more complex and will involve the following steps:

(a) The personal details of the applicant for a SID, as well as the applicant's photograph, are obtained and recorded.

(b) The applicant's documents are inspected to verify the applicant's identity, citizenship or place of residence and authenticity as a seafarer.

(c) All the information about the applicant and the application for a SID is recorded and passed to a different official of the issuing authority from the one who received the

application and recorded the data. This official then has to verify the application and authorize production of the SID.

(d) Various security checks take place. This may include checks with local police databases or with maritime schools or shipping companies to verify that the applicant is actually a seafarer. The specific checks performed vary.

(e) Once security checks are passed and authorization is received, the SID is printed.

(f) The data to be stored in the contactless chip are formatted and digitally signed.

(g) The data are written to the contactless chip and the chip is then write-protected so that no more data can be written to it.

(h) The printed SID is checked to ensure that the data are correct and that all elements have been printed correctly and are readable.

(i) The contents of the contactless chip are checked to ensure that they have been correctly encoded. This includes checking that the contents match the printed data and checking that the digital signatures can be correctly validated using the relevant public key. A failure here would mean that steps (e)–(i) need to be repeated.

(j) An entry is created in the national electronic database for the SID that was just printed.

(k) The SID is issued to the seafarer.

(l) The public keys needed to verify the authenticity of the SID are securely distributed to all authorities that may need to verify a SID. This step would only need to take place when a key is changed (every one–three months for document signer keys).

45. Once again, while all these steps may take place at the same location, they may also be divided among different locations for the sake of convenience.

46. The Ad Hoc Tripartite Maritime Committee does not have the task of providing advice or deciding on how the national issuance processes for SIDs under the proposed revised Annexes of Convention No. 185 should take place. However, three possible options in this regard are presented below in order to enable the Committee to assess the extent to which ILO Members could realistically and economically deal with the additional complexity that would be introduced by a system for a contactless chip with digital signatures and the associated PKI.

A. Production of the SID by the SID-issuing authority itself

47. This is the default option. The SID-issuing authority would perform all the steps of the process listed in paragraph 44 above. In this case, the Member would need to cover the cost of full participation in the PKD or, if possible, find another entity participating in the PKD to include the SID certificates in its Master List.

48. This would be the most expensive option, especially if a separate PKD membership was required for the SID-issuing authority. It would also be the most technically complex. There would be a potential problem in that the addition of SID-issuing authorities to the PKD might be considered a security risk. This is because the keys used to digitally sign a SID could also be used to sign an ePassport and, if they were part of the PKD, virtually no

inspection systems at border crossings would be able to judge whether the keys were being properly used. Therefore, a compromised key used by a SID-issuing authority could potentially be used to create fraudulent ePassports. There might also be a perception that SID-issuing authorities are less able to securely manage their keys and prevent fraudulent issuance than ePassport-issuing authorities. It would therefore be important for all SID-issuing authorities to clearly demonstrate their feasibility and their understanding of proper security protocols so that they would be allowed to participate in the PKD.

49. This option would, nevertheless, have several advantages. It would allow the SID-issuing authority to manage all aspects of the issuance process and to ensure that its security protocols were included in the entire process. It would also allow the issuance software and hardware to be designed and built as a unified system for the explicit purpose of issuing SIDs. This should result in an efficient and effective system that would properly address all the unique aspects of issuing a SID under Convention No. 185, as opposed to issuing an ePassport or other type of document.

50. The disadvantages would be the cost (especially of participating in the PKD) and the complexity of learning about the new technologies (contactless chips, digital signatures and the PKI) for the SID-issuing authority.

B. Production of the SID by the ePassport-issuing authority

51. One of the simplest solutions for an authority that issues SIDs in conformity with the proposed revised Annexes of Convention No. 185 would be to delegate the entire issuance process to its national ePassport-issuing authority. If the ILO Member already issues an ePassport and participates in the PKD, its national ePassport-issuing authority would have already set up the infrastructure to manage contactless chips and would have all the software and hardware required to encode them. In this case, the steps (a)–(l) listed in paragraph 44 above would be delegated to the ePassport-issuing authority. The national electronic database and the corresponding focal point might be managed by the SID authority or by the ePassport-issuing authority.

52. The main benefit of this option is that the complex task of managing digital signatures, certificates and the PKI would be performed by an entity that has already paid for the infrastructure to manage them. Since the same CSCA could be used to sign all documents issued by the same ePassport-issuing authority, there would be no extra cost or effort to manage the PKI. This could save a significant amount of financial resources for the Member concerned.

53. The ePassport-issuing authority would still need to add printers capable of handling a credit card-sized document rather than a passport book and it would need to make changes to its issuance software, in order to handle SIDs, but most of the features in the existing issuance software and in its issuance process would remain unchanged. The cost of such modifications should be much less than the cost of developing a completely new issuance system.

54. The potential drawback to this option would be the loss of control for the SID authority, since it would be delegating its functions to a different authority in the same country. There might also be difficulty in making the necessary arrangements between the two issuing authorities. Many ePassport-issuing authorities might not wish to change their software or add print capability for a different sized document.

55. There may also be some issues with staff at the ePassport-issuing authority not understanding how to properly check the documentation of a seafarer. The identity checks

and citizenship or residency checks are probably familiar, but the check to verify that the applicant is a seafarer is not something that a passport issuer would be familiar with. This difficulty could be solved, however, by a hybrid system in which steps (a), (b) and possibly (c) and (k) would be handled by the SID authority and the remaining steps by the ePassport-issuing authority.

56. In summary, this option would be both cost effective and secure, but would require internal cooperation to implement.

C. Enrolment of the seafarer by the SID-issuing authority with production of the SID being contracted out

57. With this option, the SID-issuing authority would remain in control of the issuance process, but would contract out parts of the process to an independent legal entity, thus avoiding some of the cost and complexity. Arrangements with such an entity could be made by interested ratifying Members of the ILO. The independent entity would be outside the control of any single ILO Member as it would offer its services to several national SID-issuing authorities. For the purpose of this explanation, the independent entity will be called the central processing office (CPO).

58. In this option, steps (a)–(d) set out in paragraph 44 above would be conducted by the SID-issuing authority, but instead of using its own issuance software, it would use a web-based application run from central servers. The servers would be hosted at the CPO, but the database for each issuing authority would be kept separate and private from all the others. Steps (e)–(j) and (l) would be carried out by the CPO on behalf of the SID-issuing authority. Step (k) (issuance of the SID) could possibly be performed by the CPO by directly mailing the finished SID to the seafarer or preferably be performed by the SID-issuing authority, to which the completed SID would be mailed by the CPO.

59. All the responsibility and authority for the enrolment of the seafarer, including collecting their personal data and their photograph and verifying their identity, citizenship or place of residency and status as a seafarer would remain with the SID-issuing authority as, in line with the Convention, this responsibility must remain with the State of nationality or permanent residence of the seafarer, which is the authority most able to perform the required verification. Similarly, the security checks and final decision to authorize the printing of a SID would remain under the control of the SID-issuing authority. Responsibility for printing the SID, encoding the contactless chip and managing the PKI, however, would be delegated to the CPO.

60. The advantage of this option is that the CPO would only have to develop one set of issuance software and have one set of printer and chip-encoding hardware regardless of how many ILO Members chose to use its services. Obviously there would need to be more servers and more printers added as volumes increased, but the total number of SIDs that would be issued globally in a year is quite small (perhaps 400,000–600,000) even if most of the ILO member States ratified and chose to use the CPO. This maximum possible number of SIDs issued globally in a year would be approximately the number of ePassports issued per year by a single medium-sized country. This would reduce the need for every ILO Member to incur all the expense of developing an issuance system and managing the PKI as they do for ePassports. It is also likely that a single CSCA could be used to identify all SIDs issued by the CPO for all ILO Members, with separate document signer keys being used for each individual Member. This would greatly simplify the management of the PKI.

61. A SID-issuing authority which chose this option would need to have Internet-connected computers and either cameras or scanners to capture the seafarers' facial images, but would not need any printer or chip-encoding hardware or its own issuance software. These latter items would be at the CPO. The SID-issuing authority would need at least one ePassport reader so that the data from the SID could be read and displayed for individual seafarers who wanted to exercise their right under Article 3, paragraph 9, of Convention No. 185, to inspect any data concerning them that are not eye-readable. This should result in massive savings in both hardware and software costs.

62. The SID-issuing authority would still maintain control of the data relating to its seafarers as the central servers would be maintained in a secure facility and the data for each individual issuing authority would be segregated with no access except from the staff of that authority and, for printing purposes only, the staff of the CPO. All the normal security checks could occur within the member State and the decision to approve the issuance of an individual SID would still reside with an official of the SID-issuing authority; however, the record of the approval decision would be stored on the central servers at the CPO.

63. Thus, the cost of issuing SIDs in conformity with the proposed revised Annexes of Convention No. 185 would be greatly reduced as most of the infrastructure costs would be shared by the Members that chose to use the CPO. The level of security would not be reduced and, if a reliable CPO was chosen, would probably be increased as the printing and encoding of the SIDs would take place in a secure facility staffed by personnel who would have a very small probability (due to their geographical separation) of being able to collaborate with officials of the SID-issuing authority to engage in fraudulent issuance. The management of the PKI would also be simplified, especially if the CPO used a single CSCA for all SIDs.

64. One of the disadvantages of this option would be that the SID-issuing authorities would lose any flexibility in how their issuance system operated. All those working with the CPO would need to use the same issuance system with the same protocols and the same user interface. There would probably be enough flexibility to allow minor design variations, such as national flags, in the printed SID, but most elements would have to be the same for every SID or much of the cost benefits would be lost.

65. Another disadvantage is that any automated links between the SID system and other systems which might be used for security checks (such as a national police system or an electronic database of maritime schools) would be discouraged as they would require country-specific modules to be added to the issuance software at the CPO. It is not clear if any ILO Member has implemented such automated links as part of the security checking in any of the existing SID-issuance systems, but it is important to note that such links would require extra effort and therefore cost under this option.

66. The major disadvantage with this option, however, is that it might be difficult to find any entity willing to act as a CPO. This is because the rate of ratification of Convention No. 185 and especially the rate of issuance of SIDs has been rather slow and it would be difficult for the CPO to estimate how many ILO Members might decide to use its services and in what time frame this would happen. Since the main advantage of this option is that the cost of hardware and software and PKI management would be shared among all countries using the CPO, the cost savings would be directly proportional to the number of SID-issuing authorities that decided to use the CPO. The problem is similar to the problem faced by the PKD, where the cost of participating in the PKD tends to be lower each year as more countries become participants. This effect would be magnified for the CPO as it would not simply be managing a PKI, but an entire issuance and document-production system.

67. The most realistic way of overcoming this would be for the ILO to coordinate with several interested Members until a sufficient number were found to justify the expense of creating the CPO. Then a procurement exercise could take place, led by either the ILO or by one of the Members, to find an entity willing to create and manage the CPO. The initial cost would be based on the number of Members participating at the start, with an agreement on how the cost would decrease as certain thresholds were achieved in terms of the numbers of participating Members and the number of SIDs being issued each year.

68. The concept of secure documents being printed at a shared central printing office is actually quite common. This is done for many different applications and quite a few countries even contract out their printing of stamps and currency to one of a few major security printers in the global market.

69. The concept of a shared issuance system being used by several countries is less common, but it is simply another aspect of the emerging trend to move as many IT processes as possible into the cloud. Cloud computing hosted on central servers is now used by many private companies and governments and seems to be rapidly increasing in popularity. In 2015, the first example of cloud-based issuance for ePassports took place when six United Kingdom territories began to issue ePassports using a single, shared, cloud-based system.

70. Another approach that could be adopted if the CPO existed would be for SID-issuing authorities to allow the CPO to manage their national electronic database and to support their national focal point. Since the data would still be under the control of the SID-issuing authority but would be hosted at a secure data centre managed by the CPO, it would make sense for the CPO to run a service that could provide the round-the-clock availability required by the national focal point and to take a subset of the data it hosted for the SID-issuance process and store that in a separate national electronic database for each participating issuing authority, which could then be accessed by that focal point. This could potentially save financial resources, since running a true round-the-clock contact point, as required by Article 4, paragraph 4, of Convention No. 185, is expensive, and it would also make it easier for border authorities or others seeking to verify a SID through the national focal points, since they could use the same contact details (phone number, email, URL, and so on) for all ILO Members contracting out to the CPO.

71. In summary, this option could save financial resources and involves contracting out the new complexities related to using a contactless chip in the SID and managing digital signatures and the PKD to a third party with specialized expertise in these areas. It would also create the potential to simplify the management of the national electronic database and the national focal point. Although it would require coordination among interested ILO Members to make it cost effective to set up, it would become even more cost effective as more Members began to participate.

IV. Addendum

Comments of the International Civil Aviation Organization (ICAO)

72. On 8 January 2016, the International Labour Office received comments from the International Civil Aviation Organization (ICAO) to the background paper *Commentary and draft proposals for amendments to Annex I, Annex II and Annex III of Convention No. 185* prepared for the meeting of the Ad Hoc Tripartite Maritime Committee. The comments mainly concern the cryptographic signing of SIDs when implementing the

proposed amendments. Their implications for the three options presented in Part III of the background paper may be summarized as follows:

- Option A: Production of the SID by the SID-issuing authority itself (paragraphs 47–50 of the background paper). This option would not be feasible for the ICAO unless the SID-issuing authority would collaborate with the national ePassport-issuing authority to obtain signing keys from the national CSCA owned by the ePassport-issuing authority.

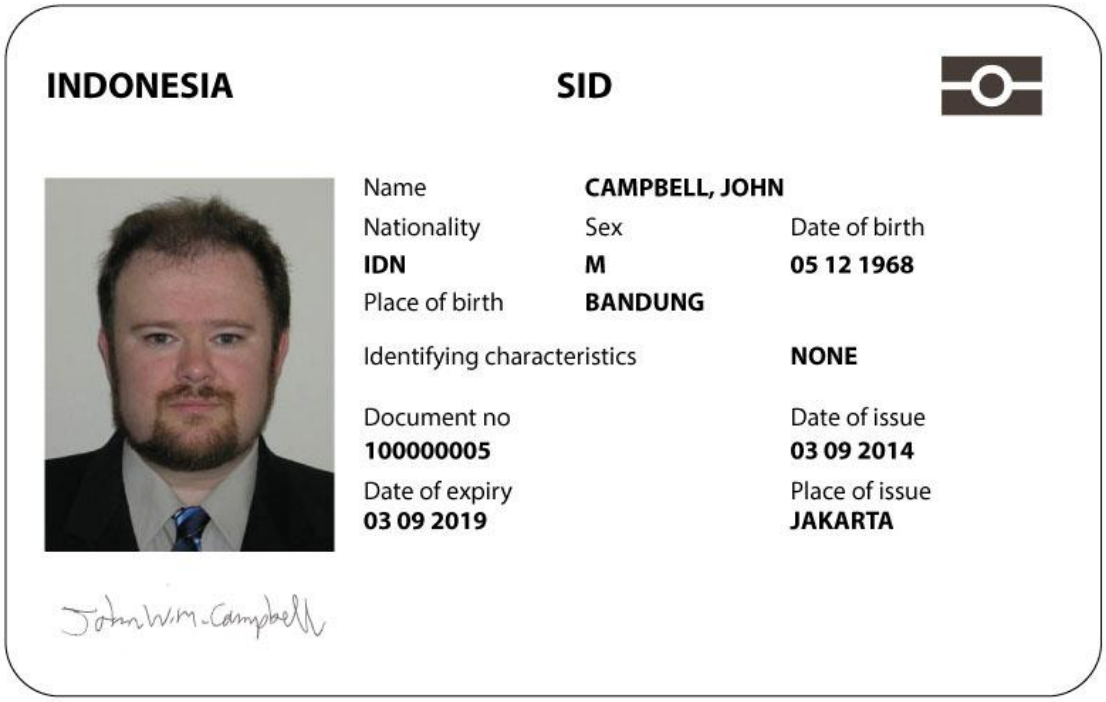
- Option B: Production of the SID by the ePassport-issuing authority (paragraphs 51–56 of the background paper). The ICAO supports option B both in the event that the ePassport-issuing authority would perform all the tasks of the document issuance process, and also if the ePassport-issuing authority and the SID-issuing authority were to share the responsibility for the different tasks, provided that the country's existing infrastructure for signing ePassports is used.

- Option C: Enrolment of the seafarer by the SID-issuing authority with production of the SID being contracted out (paragraphs 57–71 of the background paper). This option would be possible for the ICAO only if the ILO would control the CPO and collaborate with the United Nations Laissez-Passer-issuing authority to use its CSCA. For the ICAO, this option could also be used in parallel with the other options as outlined above.

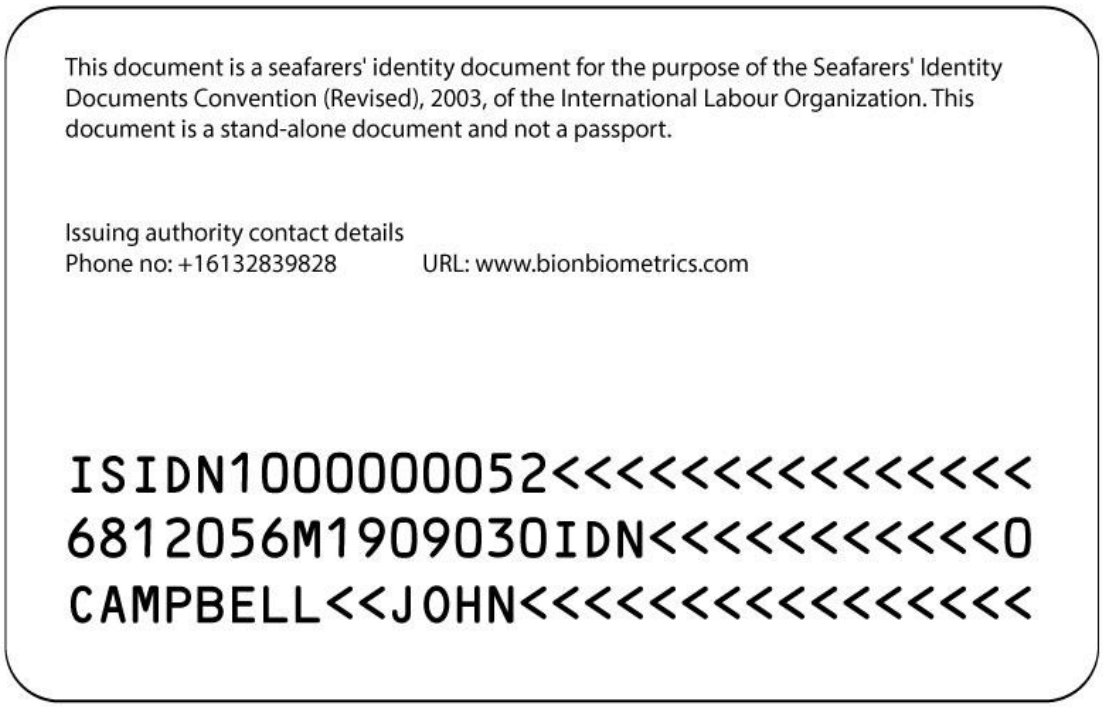
73. The Ad Hoc Tripartite Maritime Committee may wish to note that option C as reflected in the ICAO's comments would require a very careful examination of the ILO's role and responsibilities, including financial implications, and would also call for extensive consultations with the United Nations.

Appendix

Example of a seafarers' identity document prepared according to the proposed amended version of Annex I to Convention No. 185



Front



Back