INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Circ.1665
28 June 2023

GUIDELINES ON THE USE OF ELECTRONIC CERTIFICATES OF SEAFARERS

1 The Maritime Safety Committee, at its 107th session (31 May to 9 June 2023), with a view to providing a timely response to the global digitalization trend, as well as enhancing the management and control of seafarers' certificates issued pursuant to the 1978 STCW Convention, approved the *Guidelines on the use of electronic certificates of seafarers*.

2 Parties to the STCW Convention and other relevant stakeholders are invited to take full account of the Guidelines set out in the annex when implementing certification provisions in accordance with the STCW Convention and Code.

3 Member Governments and Parties to the STCW Convention are also invited to bring these Guidelines to the attention of all concerned, in particular Port State Control Officers, recognized organizations, companies and other relevant stakeholders.

4 Member Governments, Parties to the STCW Convention, international organizations and non-governmental organizations in consultative status are also invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained with the use of the Guidelines.

***

ANNEX

GUIDELINES ON THE USE OF ELECTRONIC CERTIFICATES OF SEAFARERS

Introduction

1 In recent years, substantial progress has been achieved worldwide in the field of electronic storage and exchange of information, information technology and cybersecurity. The International Maritime Organization has become increasingly involved in that global trend by, inter alia, leading work to reduce administrative burdens on seafarers and shipping companies, and encourage the use and recognition of electronic certificates, as formalized in the *Guidelines for the use of electronic certificates* (FAL.5/Circ.39/Rev.2). A number of electronic solutions aimed at improving the management and control of certificates and the seafarers' certification process already exist. There is a clear need to thoroughly address the issues related to the use of electronic certificates of seafarers pursuant to the 1978 STCW Convention and Code in order to respond to the global digitalization trend and to provide a solution for the facilitation of management and control of seafarers' documentation.

2 This document provides guidelines and information on the use of electronic certificates of seafarers.

Definitions

3 The following definitions apply for these Guidelines:

.1 *Electronic certificate* means a certificate issued in an electronic format established/approved by the Administration to ensure viewing compatibility for all intended verifiers.

.2 *Electronic signature* means data in electronic form which is attached to, embedded in, or logically associated with, other electronic data to serve as a method of authentication of the issuer and contents of the electronic data.

.3 *Unique tracking number* means a string of numbers, letters or symbols used as an identifier to distinguish an electronic certificate issued by or under the authority of an Administration from any other electronic certificate issued by or under the authority of the same Administration.

.4 *Verification* means a reliable, secure and continuously available process to confirm the authenticity and validity of an electronic certificate using the unique tracking number and other data contained on or embedded in the electronic certificate.

.5 *Printed version of electronic certificate* means a printout produced from the electronic certificate.

Verification

4 The Administration should be required to provide for the verification of electronic certificates of seafarers for all intended parties. If a remote data storage is used (e.g. server), the Administration should allow access to the appropriate data for intended verifiers on the server, and intended verifiers should provide themselves Internet access to the server. The seafarer should hold minimum required data on board, which should be defined by the Administration and would be necessary in order to initiate a verification procedure.

5 Verification may be obtained through an application, approved stored data, approved unique tracking number, approved seafarer identification number, Quick Response (QR) code, any combination of the above items, or whatever is deemed suitable for this purpose and approved by the Administration. The unique tracking number and other data for verification should always be available.

6 If the aforementioned conditions and requirements are met, and a seafarer holds an authentic and valid electronic certificate, such seafarer should be considered and treated as holding an original certificate on board.

7 The verifying party should at least have an Internet connection and the ability to read the electronic certificate file format. Ship's and company's (as defined in SOLAS regulation IX/1) means and equipment can be used for that purpose.

8 Instructions for verifying the electronic certificate, including confirmation of periodic endorsements, when necessary, should be provided by the Administration.

Security assurance

9 The procedure for the issuance, storage and means of verification of electronic certificates, as well as any certificate data exchange involving the Administration, should be developed and approved by the Administration. This procedure should include all necessary measures to be taken to ensure protection from fraud and security breaches.

Data form

10 The data form of an electronic certificate should be protected from fraudulent manipulations in a manner approved by the Administration. The electronic certificate should include an electronic signature, a unique tracking number and other data for the verification process. The data form should also ensure viewing compatibility for all intended verifiers.

11 The data form of an electronic certificate should be sufficient to ensure that all relevant information required in accordance with section A-I/2 of the STCW Code is included.

Physical location

12 The physical storage locations of an electronic certificate of a seafarer should be defined by the Administration taking into account the needs of the company and the seafarer to make it available for verification.

13 A server under the control or approval of the Administration should be recommended as the main location of electronic certificates. In this case, the Administration should allow access to the relevant data stored in the server for intended verifiers, and intended verifiers should have Internet access to reach the server.

Privacy

14 Notwithstanding that the procedure of electronic certificate verification or any data exchange should be approved by the Administration, it should also be in compliance with the Administration's law of privacy.

15 For convenience reasons, third parties, besides the Administration and the certificate holder, may be able to have access to information of the certificate, provided that it does not compromise the Administration's law of privacy.

Features

16 Administrations that use electronic certificates should ensure that these certificates have the following features:

.1 validity and consistency in line with the format and content required by the relevant international regulations, as applicable;

.2 be protected from edits, modifications or revisions other than those authorized by the Administration;

.3 be provided with a unique tracking number and other data used for verification as defined in paragraphs 3.3 and 3.4, respectively; and

.4 be provided with a visible confirmation of the source of issuance.

17 Administrations that use websites for verifying electronic certificates should ensure that these sites are constructed and managed in accordance with established information security standards for access control, fraud prevention, resistance to cyberattacks and resilience to man-made and natural disasters.*

18 Electronic signatures applied to electronic certificates should meet verification standards, as adopted by the Administration.

Notifications

19 Administrations deciding to issue or authorize issuance of electronic certificates are invited to inform the Maritime Safety Committee on their experience. All Administrations are urged to communicate to the Organization, through the relevant module in the Global Integrated Shipping Information System (GISIS), the list of certificates' categories that will be issued by the Administration or its representative as electronic certificates.

Acceptance

20 All port State control officers and relevant stakeholders should accept electronic certificates containing the features identified in paragraph 16. These electronic certificates should be verified, when necessary, following the instructions provided by the Administration (see paragraph 8).

Implementation

21 Administrations should put in place the necessary procedures in order to ensure that all related stakeholders' needs, capacities and expectations are taken into consideration before and during the implementation and use of electronic certificates.

---

* Refer to the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series standards and similar guidelines, including national requirements of the Administration.