

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

FAL-LEG-MEPC-MSC.1/Circ.1  
1 June 2026

## JOINT GUIDELINES FOR THE USE OF ELECTRONIC CERTIFICATES

1 The Facilitation Committee, at its forty-ninth session (10 to 14 March 2025), the Legal Committee, at its 112th session (24 to 28 March 2025), the Maritime Safety Committee, at its 110th session (18 to 27 June 2025) and the Marine Environment Protection Committee, at its eighty-fourth session (27 April to 1 May 2026), approved the *Joint Guidelines for the use of electronic certificates*.

2 Member States are invited to bring these Guidelines to the attention of all stakeholders concerned, in particular, those who are involved in the process of issuance, maintenance, endorsement and revision of electronic certificates included in the *List of certificates and documents required to be carried on board ships*<sup>\*</sup>, as amended, such as recognized organizations, port State control regimes, shipowners, companies and seafarers, agents and vetting companies.

3 Member States are also invited to take the necessary actions at the national level to ensure that adequate legislation is in place for the use and acceptance of electronic certificates, as may be required.

4 This circular revokes FAL.5/Circ.39/Rev.2 and MSC.1/Circ.1665.

\*\*\*

---

\* FAL.2/Circ.133; MEPC.1/Circ.902; MSC.1/Circ.1646; LEG.2/Circ.4.



## ANNEX

### JOINT GUIDELINES FOR THE USE OF ELECTRONIC CERTIFICATES

#### 1 Introduction

1.1 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.

1.2 Signed paper certificates issued by or under the authority of Governments and recognized organizations authorized to act on their behalf have been the traditional means of documenting compliance with IMO requirements.

1.3 Contracting Governments and Parties using electronic certificates, including printed versions of electronic certificates, have experienced instances of port State control officers (PSCOs) or other stakeholders questioning the validity of these certificates, resulting in additional administrative burdens for the master and crew, shipowner or operator, PSCOs, Administration and other stakeholders.

1.4 In addition, ships have experienced instances of port State control actions because a traditional paper certificate has been issued but has not arrived on the ship or has been damaged or lost.

1.5 There is also 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.

1.6 Establishing a recognized set of features for using electronic certificates should help alleviate problems inherent in reliance on paper.

#### 2 Purpose

These Guidelines provide guidance and information on the use of any kind of electronic certificates issued for the purpose of documenting compliance with IMO requirements, including electronic certificates of seafarers. However, publications, manuals, instructions or ships' logs used to record ongoing operations are excluded from these Guidelines.

#### 3 Definitions

For the purpose of 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, or 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 *Printed version of electronic certificate* means a paper version produced from the electronic certificate;

- .4 *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; and
- .5 *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 in, or embedded in, the electronic certificate.

#### **4 Features of electronic certificates**

4.1 Administrations that use electronic certificates should ensure that these certificates conform to the following:

- .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 issuer or the Administration;
- .3 be provided with a unique tracking number and other data used for verification as defined in paragraphs 3.4 and 3.5;
- .4 be provided with a visible confirmation of the source of issuance; and
- .5 include an electronic signature.

4.2 The data form of an electronic certificate should be protected from fraudulent manipulations in a manner approved by the Administration. Administrations that use websites for online viewing or 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.\*

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

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

#### **5 Verification of electronic certificates**

5.1 Instructions for verification (see paragraph 3.5) of the information contained in the electronic certificate, including confirmation of periodic endorsements, as necessary, should be available on board the ship.

---

\* Such as the International Organization for Standardization/International Electrotechnical Commission 27000 series standards and similar guidelines, including requirements of the Administration.

## 5.2 In the case of electronic certificates of seafarers:

- .1 the Administration should be required to provide for the verification of such certificates for all intended parties. If 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 can access it through the Internet. The seafarer should hold the minimum required data on board, which should be defined by the Administration and would be necessary in order to initiate a verification procedure.
- .2 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.
- .3 If the aforementioned conditions and requirements are met, and a seafarer holds an authentic and valid electronic certificate, such a seafarer should be considered and treated as holding an original certificate on board.
- .4 The verifying party should at least have an Internet connection and the ability to read the electronic certificate file format. The means and equipment of the ship and the company (as defined in SOLAS regulation IX/1) can be used for this purpose.
- .5 Instructions for verifying the electronic certificate should be provided by the Administration.

## 6 Notifications

Administrations deciding to issue, or authorize the issuance of, electronic certificates are invited to inform the Organization of their experience. All Administrations are urged to communicate to the Organization the list of certificate categories identified in the existing FAL/MEPC/MSC/LEG circular, which will be issued by the Administration or its representative as electronic certificates, through the relevant module in the Global Integrated Shipping Information System (GISIS).

## 7 Acceptance of electronic certificates

All stakeholders, including PSCOs, should accept electronic certificates containing the features identified in section 4. These electronic certificates should be verified, when necessary, following the instructions provided by the Administration available on board the ship (see paragraph 3.5).

## 8 Implementation of electronic certificates

8.1 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 of electronic certificates.

8.2 Shipowners, operators and crews on ships that carry and use electronic certificates should ensure that these certificates are controlled through the safety management system, as described in section 11 of the International Safety Management Code.

## **9 Security assurance of electronic certificates**

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.

## **10 Physical location and privacy of electronic certificates of seafarers**

10.1 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.

10.2 A server under the control or approval of the Administration should be recommended as the main location of electronic certificates of seafarers. 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.

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

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

---