INTERNATIONAL MARITIME ORGANIZATION

E

FACILITATION COMMITTEE
39th session
Agenda item 5

FAL 39/5
20 June 2014
Original: ENGLISH

E-BUSINESS POSSIBILITIES FOR THE FACILITATION OF MARITIME TRAFFIC

Report of the Correspondence Group on electronic access to, or electronic versions of, certificates and documents required to be carried on ships

Submitted by the United States

SUMMARY

Executive summary:	This document describes the work of the Correspondence Group on electronic access to certificates and documents. Annex 1 shows the draft updated interim guidelines for use of printed versions of electronic certificates. Annex 2 shows an example of a GISIS entry for using and accepting electronic certificates.
Strategic direction:	8
High-level action:	8.0.3
Planned output:	8.0.3.1
Action to be taken:	Paragraph 6
Related documents:	FAL 38/15, FAL 38/5 and FAL FAL.5/Circ.39

Background

1 FAL 38 established the Correspondence Group on electronic measures for the clearance of ships under the direction of Mr. Roger K. Butturini (United States) in April 2013. The following Member Governments participated in the work of the correspondence group:

BELGIUM
BRAZIL
BULGARIA
CHINA
CYPRUS
DENMARK
DOMINICA
FINLAND
FRANCE
GERMANY
GREECE
ISRAEL
ITALY
JAPAN
LIBERIA
NETHERLANDS
NORWAY
POLAND
REPUBLIC OF KOREA
RUSSIA
SAINT KITTS AND NEVIS
SPAIN

SWEDEN
TURKEY
UNITED KINGDOM
UNITED STATES

the following Associate Member of IMO:

HONG KONG, CHINA

the following intergovernmental organization:

EUROPEAN COMMISSION (EC)
WORLD CUSTOMS ORGANIZATION (WCO)

and the following non-governmental organizations:

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)
INTERNATIONAL ASSOCIATION OF CLASSIFICATION SOCIETIES (IACS)

2 The work of the correspondence group was guided by the terms of reference established in FAL 38/15, paragraph 5.43:

.1 collect lessons learned through implementation of the Guidelines for use of printed versions of electronic certificates;

.2 identify the stakeholders for accommodating required periodic endorsements of printed versions of electronic certificates and recommend efficient methods for handling these endorsements;

.3 continue work on online access to certificates and electronic versions of documents, including features of websites used for their access;

.4 consider the future format of the IMO Compendium on facilitation and electronic business; and

.5 report to FAL 39.

Work done by the correspondence group

3 The members of the correspondence group completed the following tasks:

.1 The correspondence group established a work schedule to advise all participants of the tasks and deadlines needed to ensure meeting due date for submitting the Report of the correspondence group to the Committee.

.2 The correspondence group discussed implementation, challenges, and the lessons learned from electronic certificates. Numerous Administrations have begun implementing procedures and processes to leverage the advantages of issuing certificates in electronic format in lieu of traditional paper.

.3 The correspondence group reviewed the interim guidelines for use of printed versions of electronic certificates (FAL5/Circ.39) to make necessary revisions based on lessons learned and the work of the correspondence group.

.4 The correspondence group identified the potential stakeholders for periodic endorsements, including Administration officials, port State control authorities, recognized organizations, ship crews, shipowners and operators, agents, and harbour and port officials. The correspondence group also discussed methods for making endorsements on printed copies of electronic certificates and the electronic certificates themselves.

.5 The correspondence group continued to examine online access to certificates and the features of websites used for access. The correspondence group confirmed the ISO 27000 series as being the dominant international standards for web site management, security, and access controls. Other national standards could apply as well.

.6 The correspondence group considered the notion of relieving the Committee of the administrative burden to maintain the technical information in the IMO Compendium on facilitation and electronic business. The discussion focused on the purpose of the Compendium, its contents, and the challenges of ensuring the EDI information in the Compendium is always up to date with the data models used for the EDIFACT versions of the FAL forms.

Findings of the correspondence group

4 In general, the members of the correspondence group agreed on the following findings:

.1 Many Administrations have plans to implement a system to issue certificates electronically. Several pilot projects are underway and Administrations continue to evaluate the efficiencies and impacts of using electronic certificates. In some cases, due to workforce implications and the scope, simplicity, and predictability of commerce, paper certificates remain the preferred means of demonstrating compliance with IMO requirements.

.2 The application and documentation of periodic endorsements remains a concern for the many stakeholders of electronic certificates including:

- administration officials from various departments with interests and jurisdiction over the arrival, stay, and departure of ships, the persons aboard, security, and the cargo;
- port State control officers (PSCO);
- vessel master and crew;
- vessel owner and operator;
- recognized organizations (RO);
- vessel agents; and
- port, harbour, and terminal authorities.

.3 Some correspondence group members share the opinion that an endorsement applied to an electronic certificate on board the vessel, including a printed version, invalidates any other copy, such as the "original" electronic version maintained by the issuer. Other members disagree with this opinion because the certificate on board the vessel is the version used to demonstrate compliance with IMO requirements and record periodic endorsements. That is, IMO requirements clearly put responsibility on the vessel and not the issuer. In the past, when only paper certificates were recognized, the issuer might have retained a photocopied, scanned, or other type of duplicate certificate for record purposes and to facilitate reissuance. The issuer of an electronic certificate, presumably, retains a copy for the same reasons. However, an electronic or paper copy kept by the issuer does not diminish the importance of the certificate on board the vessel any more than when the paper environment was standard. The electronic environment does not change the expectation that the vessel copy is the one on which PSC is based and endorsements are applied. In fact, the issuer might be unaware that an endorsement has been added to a certificate. The validity of the certificate on board the vessel is all that matters. The current requirement that instructions to validate an electronic certificate are on the vessel serves to ensure enforcement of the original details and conditions imposed by the issuer. Therefore, while the copy of a certificate retained by the issuer might not show current endorsements, it remains the basis for the certificate onboard the vessel and is likely the source of validation.

.4 The current interim guidelines do not include a requirement that the features of an electronic certificate must prevent editing or modification by anyone other than the issuer.

.5 Flag State and RO officials can endorse a printed copy of an electronic certificate in the traditional method with a signature and stamp, as appropriate. Signature devices and software also exist to affix a handwritten signature and date to the electronic certificates viewed on the vessel's computer or even through a website (see www.topazsystems.com for one example).

.6 There are numerous global standards to make web sites for access or validation of electronic certificates secure and manageable. These standards are generally wellknown to the kind of information technology experts who would typically create and maintain the means to access electronic certificates and they are applied almost automatically as a necessity for system integrity. Most of these standards were identified in document FAL 38/5 and include:

- ISO/IEC 27000 – Information security management systems – Overview and vocabulary;
- ISO/IEC 27001 – Information security management systems – Requirements;
- ISO/IEC 27002 – Code of practice for information security management;
- ISO/IEC 27003 – Information security management system implementation guidance;

- ISO/IEC 27004 – Information security management – Measurement;

- ISO/IEC 27005 – Information security risk management;

- ISO/IEC 27006 – Requirements for bodies providing audit and certification of information security management systems;

- ISO/IEC 27010 – Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications;

- ISO/IEC 27011 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002;

- ISO/IEC 27031 – Guidelines for information and communications technology readiness for business continuity;

- ISO/IEC 27033-1 – Network security overview and concepts;

- ISO/IEC 27035 – Security incident management; and

- control, and maintenance of web sites.

.7 Requirements for original versions of certificates and documents are rare in IMO provisions. A significant exception is the STCW Convention requirement that original seafarers' certificates and endorsements must be kept on board the vessel. On the other hand, the STCW Convention also requires that information on the status of seafarers' certificates and endorsements is available for validation electronically by 1 January 2017. This is an important gauge for recognizing that electronic access to crucial ship's papers already plays an important role in the maritime community.

.8 Online readers allow viewing documents such as certificates without being able to download or print (see www.realread.com for one example). HTML code to disable downloading or printing is also a means to control online access to certificates. In addition, some Administrations have simply posted the information on certificates instead of posting an image of the certificate, such as a scanned copy, to discourage fraudulent use of electronic certificates while facilitating validation.

.9 The IMO publication Procedures for Port State Control (2012 edition) defines Valid Certificates in section 1.7.11 and guides PSCOs on handling certificate issues during inspections through Chapter 2, Port State Inspections, and Appendix 1, Guidelines for the Detention of Ships.

.10 The members of the correspondence group had very little feedback on the subject of transferring maintenance of the FAL Compendium to another organization that has more general expertise and can respond to changes in the underlying EDI data models more promptly than FAL. This was primarily due to a lack of expertise in the area of EDI messages. The absence of comments and expertise from the members of the correspondence group could be taken as confirmation that the Committee, as a whole, has very little experience with data models, the minute details of EDI message implementation guidelines, and the procedures necessary

to keep the information in the Compendium current. One commenter observed that the EDI messages used in lieu of the FAL Forms are not owned or maintained by a single organization and felt IMO FAL is the appropriate unifying body to ensure IMO objectives with EDI messages are met. Another commenter observed that, alternatively, a recognized standards organization could also be the unifying body with the interested organizations participating in the technical work.

Conclusions of the correspondence group

5 In general, the members of the correspondence group concluded these results:

.1 The use and acceptance of electronic certificates is comparable to the development of EDIFACT messages to replace the paper FAL Forms. Electronic media created a spectrum of capabilities that remains today. Some stakeholders use the electronic messages and others, for a variety of reasons, do not. The Committee's responsibilities for the use of electronic certificates, therefore, should be similar:

- confirming that electronic certificates are a means of facilitation;
- developing the functional framework and appropriate standards for ensuring that confidence in electronic certificates is compatible with traditional paper certificates;
- promoting the use of electronic certificates as a means of facilitation; and
- avoiding requirements that limit the stakeholders' choices.

.2 The use and acceptance of electronic certificates is a policy issue and not a technological one. The means exist for issuing, maintaining, and validating electronic certificates in a way that is equivalent to tradition paper certificates. From the standpoint of information integrity, endorsements, and validation there are no differences between printed copies of electronic certificates and those viewed on a screen. An Administration's preference depends on not only the Administration's capabilities but also those of its fleet, PSCOs, and the other stakeholders.

.3 Compared to traditional paper, electronic certificates are susceptible to external risks that could render certificates inaccessible when needed, such as web site outages, cyber-attacks, and computer failures. Expansion in the use of electronic certificates could create a gap between those Administrations that are ready to use electronic certificates and those who are not. Therefore, an Administration, RO, or a vessel owner and crew who choose to rely strictly on electronic certificates must consider the increased potential for detrimental PSC actions under Procedures for Port State Control caused by problems accessing electronic certificates. However, this is only relevant in the case of severe technical difficulties, and PSC authorities should not otherwise discriminate between paper and electronic versions if either is presented.

.4 A crucial stakeholder for using electronic certificates is the port State, whose PSCOs and other officials must be as confident with the validity and accuracy of electronic certificates, including printed versions, as they are with the traditional paper certificates – at least until electronic capabilities progress and the stakeholders become more familiar with the procedures for using electronic certificates. The Committee should always keep this fundamental principle in mind when developing the means to facilitate use of electronic certificates.

.5 There are no technological barriers to using electronic certificates viewed on the ship's computer or other device. The certificate information is the same whether referenced on paper or a computer, and electronic endorsements can be made by the relevant PSCOs, surveyors, inspectors, and other officials. An interpretation is needed from the Committee about whether this approach of using the ship's computer or a website would meet the "on board" requirement.

.6 The Committee should take steps to create a transparent and accessible means for Administrations to record the extent and under what circumstances they will use electronic certificates for their own fleets and accept electronic certificates for vessels visiting their ports. The IMO GISIS system is a likely location for this information. (see annex 2 for the information that could be recorded in GISIS.)

.7 The interim guidelines should be updated to reflect the work of the correspondence group and the lessons learned about using electronic certificates. The updates should include:

.1 additional features to prevent editing electronic certificates by anyone other than the issuer;

.2 Administrations have the choice to accept electronic certificates either in printed format or viewed on an electronic device; and

.3 electronic records of certificates, copies of certificates, and means of validating certificates should be protected through implementation of the procedures and processes identified in the commonly accepted standards for cybersecurity.

.8 The Committee cannot react promptly to changes in the data models that support EDI versions of the FAL Forms 1 through 7 and the Security Report. A third party more involved in review and maintenance of the data models and with whom the Committee already has a liaison is a better body to maintain the Compendium under an agreement with the Committee that clearly describes the roles and responsibilities of the third party and the Committee.

Action requested of the Committee

6 The Committee is invited to:

.1 take note of the work of the correspondence group above;

.2 decide on whether to support the use of electronic certificates viewed on device screens as equivalent to traditional paper certificates and printed versions of electronic certificates;

.3 make recommendations to MSC and MEPC about whether electronic certificates viewed from a web site meet the requirements to be "on board";

.4 decide on revisions to the interim guidelines on use of printed versions of electronic certificates, FAL.5/Circ.39 (see annex 1);

.5 support development of a GISIS module for recording use and acceptance of electronic certificates (see annex 2);

.6 decide on revisions to the interim guidelines;

.7 decide on the future maintenance of the Compendium; and

.8 decide on further work on this agenda item.

***

ANNEX 1

FAL.5/Circ.39[/rev.1]
[26 September 2014]

INTERIM GUIDELINES FOR USE ~~OF PRINTED VERSIONS~~ OF ELECTRONIC CERTIFICATES

1 The Facilitation Committee, at its thirty-~~eighth~~ninth session (~~8 to 12 April 2013~~22 to 26 September 2014), approved the attached ~~interim~~ guidelines for the use of ~~printed versions~~ of electronic certificates.

2 Member Governments are invited to bring the guidelines to the attention of all parties concerned.

3 Member Governments, international organizations and non-governmental organizations with consultative status are also invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained from the use of the guidelines for consideration of action to be taken.

4 This Circular revokes FAL.5/Circ.39.

***

ANNEX

INTERIM GUIDELINES FOR USE OF ~~PRINTED VERSIONS OF~~ ELECTRONIC CERTIFICATES

1 Introduction

1.1 The Organization aims to reduce the administrative burden on Administrations, Port State Control officials, ships' crews and other stakeholders caused, amongst other reasons, by reliance on traditional paper certificates.

1.2 Signed paper certificates issued by 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 using electronic certificates, including printed versions of electronic certificates, have experienced instances of port State control officers ~~authorities~~ denying the validity of these certificates, resulting in a burden to the master and crew, shipowner or operator, port State control officers ~~authorities~~, 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 the traditional paper certificate has been damaged or lost.

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

2 Purpose

The purpose of these ~~interim~~ guidelines is to facilitate the use and acceptance ~~of printed versions~~ of electronic certificates. These ~~interim~~ guidelines ~~are limited~~ apply to the use of ~~printed versions of~~ electronic certificates and printed versions of electronic certificates.

3 Definitions

For the purpose of these Guidelines:

.1 Certificate means a document issued by an Administration that is used to show compliance with IMO requirements and used to describe operating conditions, manning requirements, and equipment requirements. The term "certificate" does not include publications, manuals, instructions, or ships' logs used to record ongoing operations;

.2 Electronic certificate means a certificate in an electronic format accessible for viewing through a website, a computer, or other digital media ~~and used to create a printed version~~;

.3 Printed version of electronic certificate means a paper ~~certificate~~ print-out produced from the electronic certificate;

.4 Unique tracking number means a string of numbers, letters, or symbols used as an identifier to distinguish a certificate issued by an Administration or its representative from any other certificate issued by the same Administration or its representative; and

.5 Validating means a reliable, secure, and continuously available process to confirm the authenticity and validity of an electronic certificate on board the ship with the ~~source issued by the~~ Administration or its representative that issued the certificate.

4 Features

4.1 Administrations that use electronic certificates ~~as the source for printed versions~~ should ensure that these electronic certificates, including printed versions of electronic certificates, have ~~include~~ the following features:

.1 validity and consistency with the format and content required by the relevant international convention or instrument, as applicable; ~~and~~

.2 with the exception of endorsements, certificates are protected from edits, modifications, or revisions other than those made by the issuer; and

.3 a unique tracking number used for validation as defined in paragraphs 3.4 and 3.5.

4.2 Administrations that use web sites for online viewing or validating 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 cyber attack, and resilience to man-made and natural disasters[1].

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

5 Validation

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

6 Notifications

Administrations deciding to issue or authorize issuance of electronic certificates are invited to inform the Committee on their experience. All Administrations are urged to record in the Organization's Global Integrated Shipping Information System (GISIS) ~~and provide~~ the list of those certificates that the Administration or its representative will issue ~~be issued~~ as electronic versions and the list of those certificates that will be accepted as electronic versions.

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

7 Acceptance

Port State control officers should accept electronic certificates and printed versions of electronic certificates containing the features identified in paragraph 4. These ~~printed~~ electronic certificates and printed versions should be validated, when necessary, following the instructions available on board the ship (see paragraph 3.5) and the guidelines in the Procedures for Port State Control.

***

ANNEX 2

EXAMPLE GLOBAL INTEGRATED SHIPPING INFORMATION SYSTEM ENTRY

United States

Certificate Name	Issued in Electronic Format	Accepted in Electronic Format	Comments
To validate certificates issued by XXXX, [contact by phone xx-xxxx-xxxx] [visit website www.xxxx.gov] and enter the tracking number shown on the certificate.			
Passenger Ship Safety Equipment Certificate	YES	YES	Issued by U.S. Coast Guard
Cargo Ship Safety Construction Certificate	YES	YES	Issued by American Bureau of Shipping
International Oil Pollution Prevention Certificate	NO	NO	Issued by American Bureau of Shipping