INTERNATIONAL MARITIME ORGANIZATION

E

FACILITATION COMMITTEE
39th session
Agenda item 5

FAL 39/INF.2
3 July 2014
ENGLISH ONLY

E-BUSINESS POSSIBILITIES FOR THE FACILITATION OF MARITIME TRAFFIC

Information paper from ISO TC8 on technical options for implementing electronic certificates

Submitted by the International Organization for Standardization (ISO)

SUMMARY

Executive summary:	Implementation of electronic certificates can be done in various ways and this document discusses some options that are already available. The document also discusses some technology and standards that are needed to support the implementation of electronic certificates.
Strategic direction:	8
High-level action:	8.0.3
Planned output:	8.0.3.1
Action to be taken:	Paragraph 3
Related document:	FAL 38/5

1 ISO TC8 has participated in the Correspondence Group on electronic access to, or electronic versions of, certificates and documents required to be carried on ships. During this period, ISO TC8 members have also participated in the EU e-Compliance project[1], one of which goals is to facilitate shipping by introducing modern information technology in complying with rules and regulations. Some of the results from this project may be of interest in the further work on electronic certificates in IMO and is therefore presented here with the permit of the project partners. The results are set out in the annex.

2 Some of the technological solutions proposed in the annex will require standardisation and ISO TC8 reiterates its availability to the Facilitation Committee if required to assist in developing such standards. Some relevant standards could be:

.1 XML formats for representation of certificate information, e.g. based on the ISO 28005 series of standards;

[1] http://www.e-compliance-project.eu/

.2 Electronic signatures for the XML file; and

.3 Standards for embedding this information including electronic signatures in QR codes.

Action requested of the Committee

3 The Committee is invited to note the information provided, and take action as appropriate.

***

ANNEX

An overview and comparison of possible technologies that can be used to implement electronic certificates.

Table of Contents

Summary

This memo discusses electronic certificates for ships and proposes a solution based on a combination of printable electronic files, e.g. in PDF incorporating an electronic signature in the form of a QR code. The code can contain machine readable information about the certificate as well as an electronic signature. The memo also proposes to add a fully electronic format, e.g. in XML to the printable format for use in fully automated processing of certificates for in-house management by ship operators or for electronic clearance of ships.

Abbreviations and definition

CeDA – Certified e-Document Authority (CeDA) refers to a trusted third party (TTP) that securely stores electronic document and certifies the contents and transmission of electronic documents for the promotion of use of electronic documents. A third party (trusted party) may be a port authority or port organization or port control (security) organization depending on IMO member states environment.

Company – The organization responsible for the management of certificates issued to a ship. This may also include certificates related to cargo, cargo carrying or crew. This may be a management company, the shipowner or others. It may also in some cases be several different organizations.

Endorsement – Two types of endorsements need to be accommodated: 1) Endorsement related to mandatory surveys or verifications during the validity period of the certificate; and 2) endorsements extending the validity of the certificate.

FS – Flag State

GISIS – IMO Global Integrated Shipping Information System[2]

PDF – Portable Document Format (Adobe registered trademark)

PS – Port State (Inspection)

QR – Quick Response (Code): Two dimensional printable and optically readable data encoding.

RO – Recognized Organization

XML – Extensible Markup Language

[2] See http://gisis.imo.org/Public/Default.aspx

1 Introduction

The certificates perform an important role in proving proof of compliance with rules and regulations or documentation that the holder is capable of performing certain operations safely and securely.

Allowing the holder to perform these operations without sufficient proof that the related requirements are satisfied can have severe costs in terms of reduced safety or security and a significantly heightened risk that the operation may result in loss of lives, health or damage to environment or property.

Delays in granting the license will also cause significant problems by hindering international trade, increasing cost of trade as well as causing lost revenue for the ship operators and cargo owners.

Thus, efficient handling of certificates is a very important part of international trade. Making use of modern information and communication technology, i.e. introducing "electronic certificates" may significant improve on the efficiency, if done properly.

This annex gives an overview of some possible methods to implement electronic access to ship certificates.

The text is structured as three main parts. Part 1 (sections 2 to 6) discusses how electronic certificates can be implemented and gives a comparison of methods and recommendations.

Part 2 (sections 7 to 10) discusses the technology that may be used to implement the electronic certificates and also suggests what standards may be needed.

Part 3 (sections 11 to 13) gives an example of how an electronic certificate could be implemented with current technology.

This document is general in nature and will not reflect all variants of how certificates are managed by various flag or port states. Some examples are also exaggerated to highlight certain problems that may occur. Thus, the document cannot be used as representing actual certificate management in the world in general or in any particular part of the world.

References to other sources or documents are given as a number in square brackets and a list of references can be found at the end of the paper.

PART ONE: POSSIBILITIES FOR IMPLEMENTATION

2 Certificate types and information contents

2.1 General type of certificates

Certificates can very generally be divided into the following categories [2].

Group	Issued by	Examples
Ship certificates	Flag State/RO	Load line, DOC, ISM
Class certificates	Class	Hull, engine, operation
Equipment certificates	Flag state/RO	VDR
Ship documentation	Owner, Builder	Stability booklet, safety plan, mandatory operational routines: SOPEP, SMPEP etc.
Log books, records	Crew/Master	Deck, engine, drills
Crew certificates	Other authorities	Master, officers and ratings, Medical
Insurance	Insurance companies	Liability, pollution
Cargo and holds	Shipper, Operator	Cargo info, DG manifest, Gas free certificate.

In general, the information that is necessary to include in a certificate is limited. The following sections will go through some types of certificates and discuss the information requirements for each of them.

2.2 Ship certificates

If one looks through the most common ship certificates, one finds that all will require all or some of the following data elements:

1. Type of certificate.
2. Certificate number or identity code.
3. Issuing organization.
4. Issued on behalf of (if issuing is RO)
5. Registry and registration code.
6. Issue date and place.
7. Valid to date.
8. Name of ship.
9. IMO number.
10. "Distinctive numbers or letters".
11. Port and year of registry.

One may also want to incorporate historic data about updates and renewals of the certificate. Note that some physical or organizational changes for the ship also will change data in the certificate descriptions.

In addition, the specific certificates will contain a few more data elements as listed below. Note that this list is not authoritative, but is intended as an example only.

International Tonnage Certificate	Length, Breadth, Moulded depth amidships to upper deck, gross tonnage, net tonnage.
International Load Line Certificate	Length, freeboard and load line for the different areas and periods relevant (summer, winter, tropical, freshwater, timber etc.).
Minimum safe manning document	Type of ship, engine room manning, type of voyages, propulsion power, gross tonnage, trading area, GMDSS sea areas, minimum manning for crew categories.
International Oil Pollution Prevention Certificate	Gross tonnage, ship type, deadweight if oil tanker.
International Sewage Pollution Prevention Certificate	Gross tonnage, maximum number of persons onboard, type of ship, type and description of sewage system.
Document of Compliance (ISM compliance for Company)	Company name and address, type of ship for which certificate is valid.
Safety Management Certificate	Type of ship and name and address of company.
International Ship Security Certificate	Type of ship and name and address of company.
International Anti-fouling System Certificate	Gross tonnage and description of system or non-application of system.
International Air Pollution Prevention Certificate	Gross tonnage.
Cargo Ship Safety Construction Certificate	Type of ship, gross tonnage and deadweight for oil tankers.

2.3 Class certificates

The general class certificate or certificates will contain much of the same information as in the previous section as well as the class notation and any relevant restriction in operation.

2.4 Equipment certificates

Equipment certificates will in general contain more technical details than the general certificates. Some examples are included below.

Voyage data recorder system-certificate of compliance	Ship type, VDR type and description, details about technical performance and inspections.
Cargo Ship Safety Equipment Certificate	Type of ship, gross tonnage and deadweight for oil tankers.
Cargo Ship Safety Radio Certificate	MMSI, Call sign, Radio equipment details.

2.5 Ship documentation

This is typically large data sets, containing drawings, safety plans, procedures etc. Inspections will verify that the documentation is on board and that it is the same as that approved by the relevant authorities.

There is a significant operational and cost gain for ship operators if this documentation can be stored electronically instead as paper. Electronic formats would also allow integration with electronic checklist systems and log books.

The verification and inspection problem is similar to that of certificates, except that the documents are extremely more bulky and that the desire to have it in electronic form only is higher.

2.6 Log books, records

Log books are similar to ship documentation, but are continuously updated with entries critical to operation. Electronic log books are already available where the logging systems themselves are approved by authorities and where checks of the logs themselves are done by checking the systems remotely or locally.

Log book and records will not be directly discussed in this paper, but some of the proposed technology is relevant also for these.

2.7 Crew certificates

Crew needs certain certificates to undertake the different critical tasks on board the ship. This is in general described in the STCW code.

Electronic certificates are different from ship certificates in that they follow crew members that go on and off the ship. Some additional mechanisms are needed to cater for this issue as, e.g. connecting them to the crew identity card.

This document does not discuss particulars of electronic crew certificates, but some of the proposed technology will be applicable also to this type of document.

2.8 Insurance

These are similar to the general certificates, but will contain additional information:

1. Owner and address (holder of insurance)
2. Insurance coverage (PI, Hull, Oil, Bunker, etc.)

Insurance documents will also vary over time and are not issued by governmental authorities. They need to be handled a bit differently than ship certificates, but some of the technical solutions for the latter may also be used for insurance.

2.9 Cargo and holds

These are specific certificates issued after certain cargo related operations have been performed, e.g. gas free certificates and clean hold certificates. They are more related to insurance documents than general ship certificates as they are issued at higher frequency and not necessarily by governmental authorities. However, the technology for implementation may be the same.

3 Requirements to electronic certificates

3.1 General operations on certificates

Related to certificates and with reference to figure 2, there are several basic operations that can be defined for certificates:

1. *Issue original certificate*: After inspection or other validation of performance or capabilities relevant for certification.

2. *Endorse certificate*: Periodically or after changes endorse certificate after a survey or other inspection, without extending validity.

3. *Endorse certificate to extend validity*: This could be done as routine or as an exceptional action to extend a certificate's validity until a new version can be issued.

4. *Reissue certificate*: A renewed version of the certificate is issued by the competent authority.

5. *Check certificate*: As part of ship clearance process or other operations, a list of certificates is checked to see if ship has appropriate certification. This may also include more extensive checks of certificate validity.

6. *Maintain certificate*: Ship operator (Company) needs to maintain list of certificates, validity and expiration dates related to each ship, with adequate consideration of trade area, type of cargo and crew.

3.2 Different information storage locations

Certificate information will in general have to be stored both onboard the ship (as a physical certificate) and in some form of central database maintained by the issuing authority. The operating company also needs to keep track of all certificates and status. In cases where the issuing authority delegates the right to issue certificates to a third party (Recognized Organization: RO), there may also be a second central database involved. This picture may also be even more complicated if a "Certified e-Document Authority" (CeDA) is charged with keeping track of the certificate status for public access.

In addition to this, the ship may also issue electronic "copies" of the certificates, e.g. a fax or a PDF file, for use in remote inspection of certificates (see section 3.4).

The main question arising out of this system is where the authoritative version of the certificate status resides. The natural may be to rely on the original stored on the ship and follow the information flow from there, but this depends on the possibility of operators to access the different databases as well as the ship documents. This is illustrated in figure 1.

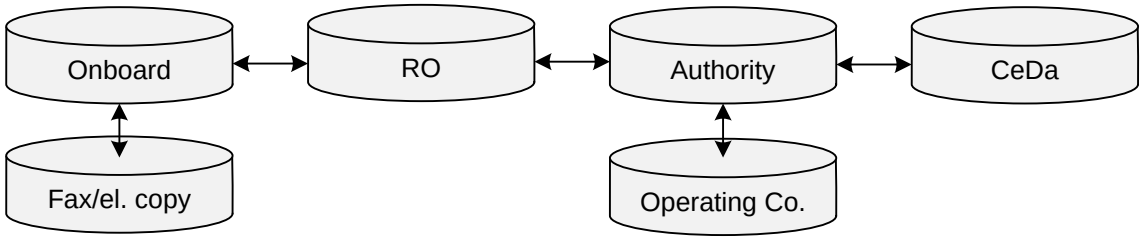

Figure 1: Certificate status code or electronic document flow

The same picture will also apply to updates in certificate status through endorsements to the certificate as well as extensions of validity resulting from endorsements (see section 3.3).

As a general rule one assumes that authoritative certificate and its endorsements are stored onboard the ship and that this is the "origin" of the authoritative certificate status. The status

will be communicated to the RO (if an RO is used) by the surveyor and then to the issuing authority which will have to maintain an updated list of certificates and their status for the ships under their flag. If a CeDA is used, this organisation will also need an updated status, either from the RO or from the authority itself.

Electronic processing of certificates can in principle be implemented by accessing certificate status in any part of this chain. The problem with this is that there is generally a time delay between the updates of the data bases for each step in the flow and one may not have access to the correct status at a given time.

Another problem is that it may be possible to forge or supress endorsed information at any stage in the chain and in particular on the original as stored onboard.

3.3 General life cycle

The issuance, inspection, endorsement, renewal and withdrawal of certificates can be said to follow a general sequence as show in figure 2. This does not include in-house management of the certificates by the Company.

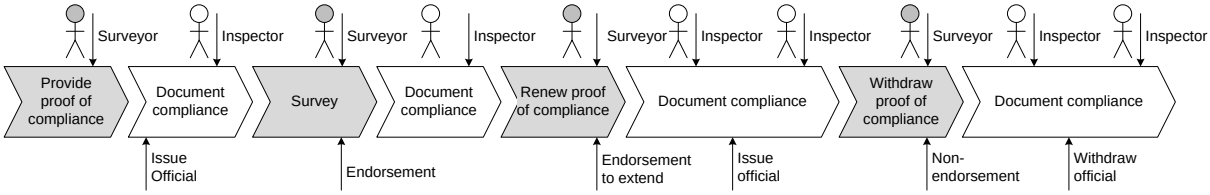

Figure 2: Generalized life cycle for certificates

In general and unless special mechanisms are mandated, there will normally be a delay between updates to the onboard certificate status and this being reflected in public or other data bases. This means that any inspector cannot necessarily rely on the data stored in the databases. It also means that if a certificate is revoked or refused endorsement before the expiration date, there may still be old "originals" onboard or in data bases that does not reflect the actual certificate status: The certificate is still valid on the old paper copy, but the actual status is that it is revoked or that it did not pass inspection.

This may be alleviated if the surveyor and the inspector both can be guaranteed to have access to the same and continuously available central data base. Otherwise, there is a potential problem of not approving a certificate that actually was renewed or, alternatively, approving a certificate that has been withdrawn.

3.4 Local or central checks of certificates

The inspector may check certificates by:

.1 going onboard to investigate the actual papers;

.2 he or she can check certificates in the office by inspecting copies of the ship papers; or

.3 by accessing a central data base.

The latter two options are preferred to speed up clearance for ships when entering or leaving port. Going on board may be necessary from time to time, but will entail delays and general slowing down of clearance as well as more work for port state officials.

However, as mentioned above, office checks of certificates may introduce new possibilities for misunderstandings or wilful forgery unless appropriate measures are taken to avoid this.

3.5 Integration with single window (SW)

There is a strong drive in many parts of the world towards making ships' port clearance electronic and more efficient through the use of single window solutions. Integrating ship certificates in the single window is a logical extension, but fully automated processing is only possible if the certificate is available in an electronically machine readable form, e.g. XML.

Much of the information in the certificates is already available from the FAL forms that are already the current basis for clearance. Thus, it makes sense to look at compatible electronic formats as e.g. the ISO 28005 series of standards for electronic port clearance [3][4]. As discussed in part three, it will be relatively easy to extend this standard to cover most of the information needed to implement electronic certificates.

3.6 Other requirements

From the above discussions there are three main problems that can occur:

.1 wilful fraud where the copy of the certificate used for inspection does not correspond to the actual compliance status. This may apply both to onboard and office inspection of certificates;

.2 not approving a certificate during inspection, as one has no access to a later endorsement that has not yet been uploaded to the data set used for verification. This may lead to unnecessary delays in clearance; and

.3 approving an invalid certificate when the certificate has been made invalid by revocation or lack of endorsement, if the new status is not yet reflected in the data set used for verification.

There are basically two issues here: 1) Establishing the validity of the version of the certificate one inspects; and 2) making sure that there is no difference between the version one inspects and the actual status of the certificate. These problems must be seen in light of the different ways to inspect the certificates:

.1 one should be able to inspect certificates on board the ship as part of, e.g. a physical port state inspection. This may relate to details in certificates not investigated in a more general office certificate checks;

.2 one should be able to inspect and approve certificates prior to ship arrival or departure to speed up port clearance processes and avoiding delays and extraneous work after ship arrival.

In addition, the system should also as far as possible simplify the process of maintaining the ship's certificate status by the operating Company. This will have the added benefit of making the general system even more attractive to the ship operators as it also gives operational benefits to their internal operation.

3.7 Summary of requirements

With the reference to the comparison table in section 5, the following requirements can be defined:

.1 it must be possible to make the issuance process as simple as possible, including the flow from surveyor, to the onboard documents and further to the shore based status update;

.2 the renewal and endorsement process must likewise be as simple as possible;

.3 the process of revoking or denying an endorsement to a certificate must also be as simple and safe as possible;

.4 the form of certificate must support avoidance and detection of fraud. It must be difficult to modify and easy to detect modifications;

.5 the form should also make it unlikely that a certificate is not accepted although the ship has passed the conformance inspections. This may happen if there are problems with communication between surveyor and issuing organisation. This may make it difficult for the inspector to access to the latest status of certificate;

.6 vice versa, it should also be unlikely that a no longer valid certificate is wrongly accepted;

.7 it should be possible to perform safe and secure inspection based on information in port officers' offices. This will reduce the delay for clearance of ship;

.8 it should be possible to perform safe and secure inspection onboard the ship, based on local information stored on the ship;

.9 in exceptional cases, it should be possible to perform safe and secure inspection in both above locations without access to Internet or to a central data base;

.10 the complexity of the certificate management system maintained by the issuing organisation should be minimized to reduce investments and operational costs for the data server system;

.11 it should be possible to integrate automatic check of electronic certificates in a single window (SW) system. In this case the ship or the agent can submit relevant certificate information through the single window; and

.12 the certificate format should also support simple management of the ship's certificates by the Company.

4 Electronic certificate implementations

4.1 PDF with stamp and signature

The traditional certificate can be implemented as, e.g. a PDF file that can be printed out on demand or transferred from the ship to shore by electronic mail or other means. Main workflow could be as described below. Without any form of unique signature on the

document, it is not possible to protect efficiently against fraud, unless a central database is used for validation.

Survey and approval	On board, surveyor register approval at own PC or sends email to central office.
Initial issue	A new electronic certificate is issued as a PDF file as well as paper.
Renewal and endorsement	By signature on paper. Not possible to transmit to shore other than as fax.
Revoking certificate	Only in central office, old certificates may be onboard until expiry.
Inspection on ship	Manually check paper copy and signatures.
Inspection on shore	Manually check PDF/fax with signatures.

As multiple copies of the electronic certificate may exist, one cannot rely on deleting the file when one revokes the certificate.

4.2 Paper with QR code

One may also additionally sign the PDF certificate with an electronic signature embedded in a QR code in the PDF.

Using a QR code would make it possible to verify authenticity by an offline application on a mobile unit, e.g. PC or mobile phone, even by investigating the paper copy alone. In this case, the QR code would contain a signature code as well as code referencing the issuer, e.g. through the IMO GISIS system. However, the validation would be sensitive to wilful forgery, e.g. by changing text in certificate before copying in a valid QR code.

The QR coded signature can cross check all data on the certificate, but unless this data is also available as electronic information, it is difficult for the inspector to verify that the data is correct.

The work process is outlined below.

Survey and approval	On board, surveyor register approval at own PC or sends email to central office.
Initial issue	A new electronic certificate is issued as a PDF file with a QR code. No paper copy is needed.
Renewal and endorsement	The endorsement should normally be given as a new electronic QR on the same certificate, issued from central office or surveyor. Alternatively or in addition, a normal endorsement signature can be added to a paper document. This will not be electronically transferrable to shore, other as a traditional fax until the new electronic version has been received.
Revoking certificate	Immediately in central database, but old certificate copies can still be falsely used until expiry date, unless checked against central database.
Inspection on ship	Can be verified automatically and by checking key data elements manually (ship identity and expiry date). Otherwise have to rely on manual inspection of paper copies.
Inspection on shore	Same as on board, but less secure with respect to faxed documents when electronically are not yet available.

4.3 Paper with electronic signature and central check

If a QR code is used, it can also embed a reference to an online resource that can further verify the status with respect to pending revoking or renewing the certificate by accessing a central database.

PDF also supports embedded electronic signature of documents and this may be used in this case. PDF signatures must be validated through the Internet so access to the net is necessary for proper validation.

Note also that Adobe support local *issuing* of new certificates by using certification keys stored on protected USB hardware devices. This can be used for immediate issue of endorsements or for renewals as new printable PDF files. This is a safe method that can be used to avoid forgery or loss of certification codes. However, use of the Adobe mechanisms for issuing certificates requires a paid for license from Adobe.

The Internet address for validation should not be embedded in the QR directly as that may be used to fake the Internet verification process. The QR should contain a reference code, e.g., using the IMO GISIS database as repository that points to relevant data for authentication. This means that the surveyor needs to download data from GISIS during or before the inspection of the certificate.

The surveyor needs to be able to access the central repository to execute the verification. This requires online access to Internet.

One needs to create some safe-guards related to protection of keys for the signature creation. This means that the generation of the signature should not be done locally by the surveyor, but done by the central data system. Alternatively, one may rely on a hardware protected USB type key device that the surveyors will get from the issuing authority. Several certification codes can be stored on the same physical device.

Survey and approval	On board, surveyor register approval at own PC or sends email to central office. A new certificate can be generated immediately or after a short processing time.
Initial issue	Immediately or after a short delay from survey. Electronic issue only.
Renewal and endorsement	As new electronic file that can be generated immediately from central server, but can use paper copy if necessary.
Revoking certificate	Immediately in central database. Old certificate copies cannot easily be used.
Inspection on ship	Can be verified automatically against central database.
Inspection on shore	Can be verified automatically against central database.

The central check will require access to Internet and the central data base, but lack of this would still not make this method less certain or simple than checking paper based certificates.

4.4 Electronic document available from FS/RO Internet site

The actual electronic certificate can also be made available from a secure web service maintained by the flag state or the RO. Any inspectors would then need to be able to access this data base. This will further minimize or remove the time gap between inspection and time when the centrally issued certificate is updated. By accessing the data base, one would always get access to the most updated version. However, it depends on the maintaining organization being able to keep the delays at a minimum and also to make sure that the data base is available at all times.

Having an electronic version on the certificate onboard the ship and in the management office would also act as backup in the rare cases where the central data base is not accessible.

Use of the system will be as for the previous section, but it may be somewhat more complicated to handle paper backups. The inspector would also need to have and maintain credentials for the specific certificates in the Organization's data base.

For the responsible organization, this is not significantly different from the alternative presented in the previous section. The PDF needs to be available in addition to the authentication function, but authentication is probably sufficient in the centrally stored PDF itself.

4.5 Use of CDeA

The use of a central repository for electronic certificates has some benefits:

.1 the flag State administration or the RO do not have to implement an own data base with sufficient reliability for general use. They can use a trusted third party and reduce implementation and operational costs; and

.2 it provides a central repository for ship certificates independent of one having the exact information related one specific ship or flag state. However, if the certificate has a QR-code, this is less of an issue.

The draw-back of this solution is of course to determine how the implementation and operational costs shall be divided as well as introducing some additional delays and complexity in the work processes.

Equasis[3] is already operating a similar service for port state control, including already extensive certificate information, and could be upgraded to provide a more general certificate validation service.

Work processes will be the same as for the previous solution. A minor improvement would be that certificates would be available from one server, independent of who issued the certificates.

4.6 Use of electronic formats, e.g. XML

The certificate could also be issued as a fully electronic "message", e.g., in XML format. In this case it would need to contain the same information as in the paper certificate as well as a proper digital signature verifying the correctness of the data. The XML message could also contain information as discussed previously, e.g. reference to a verification data server.

The electronic certificate could also be implemented as a printed document with a QR code containing all the XML data elements as well as verification sources. This would allow ships to operate with printed documents for rare cases where no electronic processing is available and also get all benefits of having electronic verification and processing available.

Electronic certificates of this form would also simplify management of certificates by the responsible operators. The data could be transferred directly into databases or management software systems. This would make it much easier to keep track of all certificates, send them to agents when necessary and to keep an overview of renewal and expiry issues.

[3] http://www.equasis.org/EquasisWeb/public/HomePage. Port state inspection MoU data base.

Another benefit of a fully electronic certificate is that it can be automatically processed by port state data systems, e.g. as part of the local single window implementation.

The work processes will be identical to those listed for section 4.3 with additional benefits as indicated above.

5 Comparison of methods of electronic access

The below table has one column for each of the discussed solutions for electronic certificates with the first column representing the traditional paper based certificates. More details of the certificate solutions can be found in the corresponding subsections. Each row corresponds to one of the requirements listed in section 3.7.

Each cell has then got an indication of how well a specific certificate type satisfies the corresponding requirements. Scale is from "--" as none at all to "++" as very well. The traditional certificate can be used as reference.

	Traditional paper	**Printable on board**	**Printable with QR**	**Printable with QR and central check**	**Centrally available certificate with QR**	**Use of CeDA**	**XML coding added**
Issue certificate	-	-	-	++	++	++	++
Issue renewals	-	-	-	++	++	++	++
Revoke	-	-	-	++	++	++	++
Counter fraud	--	--	-	++	++	++	++
Wrong denial	-	-	-	++	++	++	++
Wrong acceptance	-	-	-	++	++	++	++
Check on shore	-	+	+	++	++	++	++
Check on ship	+	+	+	++	++	++	++
Internet access	++	++	++	+	+	+	+
Complexity	++	++	+	-	-	+	-
SW integration	--	--	-	-	+	+	++
Management	--	+	+	+	+	+	++

6 Summary and recommendation

Electronic certificates are certainly possible and as will be discussed in the coming sections, much of the required technology and standards are already available.

One should also observe that the different options discussed here are modular in the sense that one can select different options or build improved services without losing functionality.

The Adobe electronic signature is well suited to the problem of electronic certificates and contains most functionality one needs. However, it has some cost implications for the users.

Another attractive option would be to create a gradual implementation of electronic certificates by going through the following steps:

.1 Printable PDF with embedded QR, where the QR code contains enough information to ensure a reasonable verification of key values on certificate (expiry dates, IMO number, key elements of certificate terms). Use signature keys available from IMO GISIS for validation. This can be

implemented by the flag states that wish to. A paper copy can be printed out and kept as backup on the ship in case the electronic systems fail.

.2 Develop XML format for electronic certificate information and sign that with electronic signature as used in QR code above. This file can then be used in single window clearance in ports where the format is accepted. Inspectors on the ship can also use this format if they want to. Electronic formats with signature simplify process of checking certificates. This will be an addition to the printable certificate.

.3 Extend QR code to also include data from the XML file. Inspectors can then scan and validate the data without direct access or use of the XML file. This will also be a backup solution to a fully electronic processing in cases where Internet access or servers are unavailable.

.4 Implement individual or centralized repository for current electronic certificates in XML and printable formats, with appropriate signatures for validation. This can be the main mechanisms for maintenance and inspection of certificates. Mechanism in point 3 will act as backup for server or Internet failure.

Neither of these steps will require that all flag states implement the solution. It will provide efficiency gains for those that do and will allow a phased implementation in cases where some states need to use more time on the issue.

The critical issue is to agree on common standards so that implementation can start where it is possible and desirable.

PART TWO: TECHNICAL DETAILS

7 Electronic signatures

RSA encryption[4] forms the basis for most of the world's secure communications, including on the Internet.

The encryption uses asymmetric cryptography, and is based on a class of mathematical problems for which it is hard to find solutions, but easy to verify the solution. The classical example of this kind of problems is prime factorization: Given a number N which is a multiple of two primes. The time to find the primes will increase with the square root of N as N increases; however, if one of the primes is known, finding the second will be a near instantaneous task.

In asymmetric cryptography, a pair of separate but mathematically linked keys is generated. A public key is used to encrypt plain text or to verify a digital signature, while a private key is used to decrypt the ciphered text or to sign a document digitally. The mathematical link between the keys is created in a way that it is impossible or extremely difficult to calculate the private key from the public key. Typically the public key is made available for all relevant parties, while the private key is kept secret.

For regular encryption, this means that anyone with access to the public key may encrypt a text, but only the holder of the private key can decrypt the text; for signing, only the holder of the private key can create a valid signature, but anyone with access to the public key may verify the signature.

7.1 Hash Function

A hash function[5] maps an arbitrary string of data into a fixed length output. A "good" hash function has the following three properties:

.1 It is impossible to recreate the original data from the Hash – it is not invertible.

.2 Any change in the underlying data will produce a change in the Hash function.

.3 It is deterministic – hashing the same data again will produce an identical string. (Compare to padding functions, which are typically non deterministic).

Condition two is impossible to obtain exactly if the size of the hash function is smaller than the total variation of the data, as at least some changes must be mapped to identical hashes. However, in practice, for an appropriate choice of hash function, it is inconceivable that anyone could make a desired change to the underlying data without altering its hash.

4 http://mathworld.wolfram.com/RSAEncryption.html

5 http://mathworld.wolfram.com/HashFunction.html

7.2 Digital Signatures

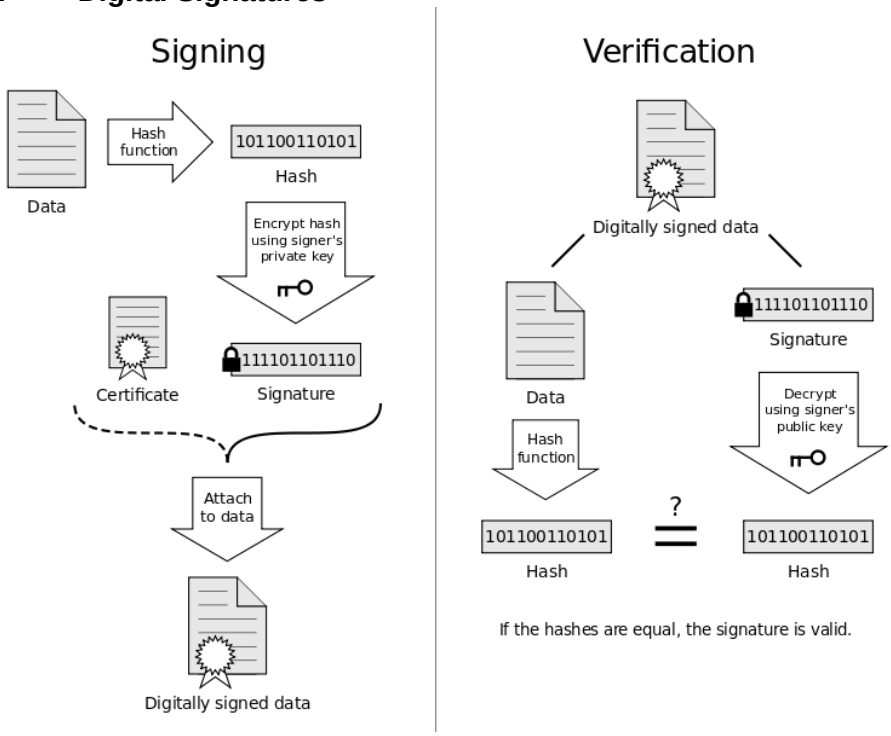

Figure 3: Diagram showing the creation and verification of a digital signature. Source Wikipedia Commons, Author Acdx

It is now common for documents to be digitally signed. This is done using RSA cryptography and hash functions. In order to be able to verify the sender and the validity of a document, a hash function is used and a RSA key pair is generated; the sender and receiver knows the hash function and the public key, while only the sender has access to the private key.

The document text is passed through the hash function, generating a string of typically 1024 bits. This string is then run through the RSA decryption algorithm, using the sender's private key. This generates a new string which is appended to the document as a signature.

As the hash function and public key is known to the receiver, the signature can be run through the RSA encryption algorithm and compared to the hash of the received document. If the hash of the document is equal to the encrypted signature, the signature is valid and the document has not been changed since the signature was added.

7.3 Electronic Signatures on Paper

In the above description, we casually assumed that "the text of the document is passed to the hash function". To sign a paper document, this might mean that someone has to manually enter all the data. That would not be an acceptable solution; however, there are a variety of ways to store information on paper in a machine readable form. The most common way is the barcode, which is slowly giving way to matrix codes like the QR code[6]. A QR code can be used to encode all the information on a certificate as plain text with addition of the signature of the issuer. Most certificates contain limited information (most of the text being standard text present on every certificate) and QR codes can take up to around 3000 characters or bytes, which should be sufficient. This is further discussed in section 8.

6 http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid=4802

The QR code containing the entire signed digital certificate can be added to the paper version of the certificate; this can then be read and authenticated by any smart phone or similar device. The issuer can issue a new certificate securely by email or can do it instantaneously on board the ship, and it can be printed and stored on board. Due to the digital signature validation, holograms and physical embossments on the paper is not necessary. The information on the paper version will be for record keeping and can also help the captain or the management company keep track of the certificates. The certificate's validity can be checked by scanning the QR code, and as it is digitally signed, further validation is not necessary.

The reviewer should never look at the information on the paper version, as the securely signed version is available as soon as the QR code is scanned. Of course, one might check that the electronic version is identical to the paper version, but in effect, the paper is just a print of the electronic version.

There is no need to regard the electronic and paper versions as in any way different. If the paper document is available, the QR code can be scanned to get the electronic version; if the electronic version is available, this can be printed complete with the QR code.

7.4 Key Security

An encryption system is only as secure as its private encryption key. However, it is not necessary to have only one key. An issuer could change their private key every day, publishing a new public key, and the application which authenticates the information just has to use the right public key by looking up the key used on the date of issue of the certificate.
It is also possible to require that the key is stored on a special hardware device, e.g. a USB unit, and further protect it by personal passwords for each user. Only the issuer of keys can write to the device and only the user knowing the password can use the key it to sign certificates.

A digital signature can also be used to authenticate other issuers. For instance, a flag State may delegate the management of certificates to some other entity. This can be done by using a mechanism similar to public key certificate[7] which is commonly used on the Internet.

The flag State creates a key pair and digitally signed certificate which is used to validate other certificate issuers. The entity with the right to issue certificates creates their own key pair and signed certificate. The entity's certificate is then signed by the flag State, using the flag State's certificate and private key. This certificate is then used for signing when the entity issues a certificate for a ship.

This creates a validation path; the flag State's original certificate and public key can be used to verify that the certificate for the ship has been issued by an entity with the right to do so.

The certificates for validation of other issuers should be issued with a relatively short expiry date, because while it is impossible to revoke a valid certificate, a certificate becomes useless after a certain date and will no longer be useful for creating further certificates.

These validation key chains mean that new certificates can be issued locally, because each party has their own certificate and their own key. There is no need for the flag State to share their private key with any parties, and it should be a closely guarded secret and changed regularly. They only need to sign the certificates of their delegation authorities, and in the event of fraud it provides a chain of liability conceivably right down to the individuals who authorized the signing of particular certificates.

[7] See http://en.wikipedia.org/wiki/Public_key_certificate

7.5 Implementation

All the technology that is needed for implementation already exists and is in common use. OpenSSL[8] will allow the creation of digitally signed certificates, and can be used to provide digital signatures to a document. Open source software to translate text into QR codes and back again already exists. All that is required is an App which displays the information in the QR code in a readable format, and makes use of OpenSSL to validate the signatures.

7.6 Revoked Certificates

A digital signature only protects against a certificate being fraudulently issued or fraudulently altered since it is impossible to revoke a properly signed digital document (although the signature may expire). If it is suspected that a certificate might have been revoked, the issuing authority, who must keep records of revocations, must be contacted. However, this should be relatively rare. In any event, most places in the world have internet, and it is a relatively simple task to look up an online database to make sure that a certificate with a valid certificate has not been revoked. This would be an extra service. Even in areas or ports where one cannot obtain internet access, it would be a relatively simple task for an app to store the certificates that it validated until such time as it was connected to the internet, at which time it could inform the user if any of the certificates that were digitally signed have since been revoked.

7.7 Conclusions

We then propose the following – that each certificate be printed with a QR code, or other machine readable format, which is not just the digital signature, but actually the entire digitally signed electronic version, including all the information. Digital signatures need not be long, although it may not be possible to store the entire validation chain on the QR code, it can at least store the digital certificate of the direct issuer.

8 QR code

QR (Quick Response) code is a type of two-dimensional barcode designed by Denso Wave, originally for use in the Japanese automotive industry. The use of QR code has quickly gained popularity in both commercial and non-commercial applications, as they can store a fairly large amount of data and can be scanned and decoded with commonly available equipment, e.g. a mobile phone equipped with a camera.

There are four encoding standards for the QR codes; numeric, alphanumeric, byte/binary and Japanese characters. Extensions may also be used. The encoding affects how much data can be stored in the code, as the number of bits used per character is dependent on the encoding.

QR code also has error correction based on the Reed-Solomon algorithm. Because of this, the data stored in the code can be reconstructed even if parts of the code have been destroyed, is dirty or overwritten. The error correction is of variable level; a code with low error correction can store more data, but will be less robust to damage than a code with high error correction.

[8] The OpenSSL Project is a collaborative, open source project to develop a robust, commercial-grade, full-featured toolkit. It is widely used throughout internet security, and is the de facto standard implementation. Their website is at http://www.openssl.org/

The QR code is of variable size, ranging from 21x21 modules[9] for version 1 to 177x177 modules for version 40.

The maximum amount of data that can be stored, e.g. in a version 40 QR code with low error correction, is 7089 numeric characters, 4296 alphanumeric characters, 2953 bytes or 1817 Japanese characters.

Due to the nature of the data in the certificates, it would be reasonable to use either alphanumeric or byte encoding. The alphanumeric encoding has some limitations, like upper-case letters only and few special characters; these limitations are inconvenient with XML style text and standard representation of encrypted signatures and key data. It would therefore seem like the byte encoding is best for the purpose of representing the certificate data.

9 Electronic certificate data in ISO 28005 compliant format

There are many certificates and documents the ship has to carry on board and it will be necessary to analyse the actual encoding requirements in detail before one decides how to encode all this or rather the necessary parts of this information in electronic documents.

However, the core information needed by surveyors is not normally that extensive and some examples are giving in part three of this paper. Almost all information elements are already available in ISO 28005-2 [4] and it is simple to create a new part of the 28005 series covering electronic certificates. This would also ensure compatibility and semantic interoperability with other electronic reporting systems using this standard or standards that have a semantic mapping to ISO 28005.

10 Need for standards

International standards will be necessary for the efficient implementation of electronic certificates. Issuer, user and inspectors must all agree on the format used and the same format should be used for all nationalities. The below table lists the main standards that are necessary and suggests who can develop these standards.

IMO means that the specifications are of a policy related nature and need to be agreed on by legislators and users represented in IMO. IS means that the specifications are technical in nature and can be developed by international standards organisations, typically ISO based on performance requirements from IMO.

Required data content in each document	IMO
Performance requirements for producing and inspecting the documents	IMO
Performance requirements for central repository of keys and documents	IMO
Digital representation of data elements in XML or other formats	IS
Methods for signing documents (from performance standards)	IS
Methods for printing data and signature on paper documents	IS
Access methods for central data bases	IS

[9] A "module" is a light or dark square, and is the smallest element of a QR code.

PART THREE: AN EXAMPLE

11 Sample certificate printed format

CERTIFICATE OF INTERNATIONAL REGISTRY

Particulars of ship

Name of ship	M/S Ship of the future		
Official Number	986714	**Year / port of registration**	2009, Hometown
Radio call sign	A14G5	**IMO Number**	9988776

Type of ship	General cargo	**No of decks**	1
Type of propulsion	Motor ship	**Details**	Single screw
Country built	Sweden	**Keel laid**	2008
Material in hull	Steel	**Overall length**	82.5 m
Stern	Raked	**Length at waterline**	80 m
Stern	Transom	**Breadth**	12 m
Moulded depth	6.5 m	**Moulded draught**	5.8 m
Yard	Shipbuilders AB, Gothenburg		

Particulars of Propelling Engine

No of sets engines	1	**Type engine**	Internal combustion
No of shafts	1	**Power**	1 400 kw
Year of build	2006	**Cylinders per set**	6
Length of stroke	400 mm	**Diameter cylinder**	300 mm
Estimated speed of ship	16 knots		
Engine maker	Hansen Maskinfabrikk AB		

Particulars of Tonnage

Gross tonnage	12 000 tons	**Net tonnage**	10 000 tons
Registered tonnage	12 000 tons		

Certificate issued to owner:	Shipholding Ltd 23 Great road Sea village, UK

Issued at and date	Hometown, Some state, July 23rd 2013
Expires at	July 22nd 2015

Signature – Stamp/Seal	

12 XML encoding

The below listing show how the same information as is represented in the printed document in section 8.1 can be encoded in XML. The format is based on the ISO 28005-2 standard for electronic port clearance, but with additional elements added to cover the needs of the certificate data set. The XML file amounts to about 3.5 kilo-byte which is not within the capacity of the QR code. Section 8.3 shows how one can construct a simple text based encoding of the XML that reduces data set size to around 1 kilo-byte. Alternatively, one could also compress the XML-file which will typically reduce it to about 1.5 kilo-byte.

```
<?xml version="1.0" ?>

<EPCElectronicShipCertificate
    xmlns="http://e-certificates" Id="986714-10-02"
    xmlns:epc="http://www.iso.org/28005-2"
    targetNamespace="http://www.iso.org/28005-2">
  <EPCCertificateHeader>
    <CertificateCode>RegistryCertificate</CertificateCode>
    <OfficialNumber>986714</OfficialNumber>

    <ShipID>
      <ShipName>M/S Ship of the future</ShipName>
      <IMONumber>9988776</IMONumber>
      <CallSign>A14G5</CallSign>
    </ShipID>

    <IssuedTo>
      <Name>Shipholding Ltd</Name>
      <PostalAddress>
         <StreetName>Great road</StreetName>
         <StreetNumber>23</StreetNumber>
         <CityName>Sea village</CityName>
         <Country>UK</Country>
      </PostalAddress>
    </IssuedTo>

    <IssuedBy>
      <Name>International ship register</Name>
      <CityName>Hometown</CityName>
      <Country>XX</Country>
      <GISIS>12345</GISIS>
    </IssuedBy>

    <IssueDate>2013-07-23</IssueDate>
    <ExpireDate>2015-07-22</ExpireDate>

    <Version>1</Version>
  </EPCCertificateHeader>
  <EPCCertificateBody>

    <RegistrationPort>
      <Name>Hometown</Name>
      <Facility/>
      <CountryCode>XX</CountryCode>
      <UNLoCode>HOM</UNLoCode>
    </RegistrationPort>

    <ShipBuilder>
      <Name>Shipbuilders AB</Name>
      <RegistrationCountryCode>SE</RegistrationCountryCode>
    </ShipBuilder>

    <ShipDescription>
      <ShipTypeContent>50</ShipTypeContent>
      <Decks>1</Decks>
      <KeelLaid>2008</KeelLaid>
      <HullMaterial>Steel</HullMaterial>
      <Speed>16.0</Speed>
      <Comment>Stern Raked, Transom</Comment>
    </ShipDescription>

    <PropulsionDescription>
```

```
      <PropulsionType>Motor</PropulsionType>
      <PropulsorType>SingleScrew</PropulsorType>
      <SetOfEngines>1</SetOfEngines>
      <Shafts>1</Shafts>
      <EngineSet>
         <EngineType>InternalCombustion</EngineType>
         <Power>1400</Power>
         <BuildYear>2006</BuildYear>
         <Cylinders>6</Cylinders>
         <StrokeLength>0.4</StrokeLength>
         <Diameter>0.3</Diameter>
         <EngineBuilder>
           <Name>Hansen Maskinfabrikk AB</Name>
           <RegistrationCountryCode>SE</RegistrationCountryCode>
         </EngineBuilder>
      </EngineSet>
    </PropulsionDescription>

    <LengthOverall>82.5</LengthOverall>
    <LengthWaterline>80.0</LengthWaterline>
    <Beam>12.0</Beam>
    <MouldedDepth>6.5</MouldedDepth>
    <MouldedDraught>5.8</MouldedDraught>

    <GrossTonnage>12000</GrossTonnage>
    <NetTonnage>10000</NetTonnage>
    <RegisteredTonnage>10000</RegisteredTonnage>
  </EPCCertificateBody>

  <s01:Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
                 xmlns:s01="http://e-certificates"
                 s02:Id="Id-BC0B1674-758D-40B9-84BF-F7BAA3AA19F4"
                 xmlns:s02="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
      </CanonicalizationMethod>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
      </SignatureMethod>
      <Reference URI="#986714-10-02">
         <Transforms>
           <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
           </Transform>
           <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml1317c14n-20010315">
           </Transform>
         </Transforms>
         <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
         <DigestValue>FHwW2U58bztLI4cIE/mp+nsBNZg=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>MTha3zLoj8Tg content omitted</SignatureValue>
    <KeyInfo>
      <X509Data>
         <X509Certificate>MIICnDCCAYQCAWUwDQYJ content omitted</X509Certificate>
      </X509Data>
    </KeyInfo>
  </s01:Signature>

</EPCElectronicShipCertificate>
```

13 Compressed plain text format

QR codes can contain up to 4296 alphanumeric characters or 2954 bytes. There are various ways to compress the data set shown in section 8.2 and in this section, a simple text encoding scheme is demonstrated. This can be used to retain all information while also making it easy to access without direct electronic compression. However, this is just one possible way to do this.

```
ec:
:ch:
::cc:RegistryCertificate
::on:986714
::si:
:::sn:M/S Ship of the future
:::in:9988776
:::cs:A14G5
::it:
:::na:Shipholding Ltd
:::pa:
::::sn:Great road
::::so:23
::::cn:Sea village
::::co:UK
::ib:
:::na:International ship register
:::cn:Hometown
:::co :XX
:::gi:12345
::id:2013-07-23
::ed:2015-07-22
::ve:1
:cb:
::rp:
:::na:Hometown
:::cc:XX
:::ul:HOM
::sb:
:::na:Shipbuilders AB
:::cc:SE
::sd:
:::st:50
:::de:1
:::kl:2008
:::hm:Steel
:::sp:16.0
:::cm:Stern Raked, Transom
::pd:
:::pt:Motor
:::pr:SingleScrew
:::se:1
:::sh:1
::es:
:::et:InternalCombustion
:::pw:1400
:::by:2006
:::cy:6
:::sl:0.4
:::di:0.3
:::eb:
:::na:Hansen Maskinfabrikk AB
:::cc:SE
::lo:82.5
::lw:80.0
::be:12.0
::me:6.5
::mr:5.8
::gt:12000
::nt:10000
::rt:10000
:si:
::dv:FHwW2U58bztLI4cIE/mp+nsBNZg=
::sv:MTha3zLoj8Tg content omitted
::ki:
:::cv:MIICnDCCAYQCAWUwDQYJ content omitted
```

References

[1] Report of the Facilitation Committee on its Thirty-Eight Session, International Maritime Organization, London, FAL38/15, May 2013.

[2] Revised List of Certificates and Documents Required to be Carried On Board Ships, International Maritime Organization, London, MSC/Circ. 1151, Dec. 2004.

[3] ISO 28005-1:2013 Security management systems for the supply chain – Electronic port clearance (EPC) – Part 1: Message structures.

[4] ISO 28005-2:2011 Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements

[5] ISO/IEC 18004:2006 Information technology – Automatic identification and data capture techniques – QR code 2005 bar code symbology specification.