Electronic certificates for ships: a LOFTY (legal, operations, fraud, trust) analysis

Bridget Cosgrave

Follow this and additional works at: https://commons.wmu.se/all_dissertations

Part of the Operations and Supply Chain Management Commons

Recommended Citation

https://commons.wmu.se/all_dissertations/654
ELECTRONIC CERTIFICATES FOR SHIPS

A LOFTy (Legal, Operations, Fraud, Trust) Analysis

By

BRIDGET PATRICIA COSGRAVE, BA Hons, MBA
Ireland / Canada

A Dissertation submitted to the World Maritime University in partial fulfilment of the requirements for the award of the degree of

MASTER OF SCIENCE

In

MARITIME AFFAIRS
(MARITIME LAW AND POLICY)

2018

Copyright: Bridget Cosgrave 2018
Declaration

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature): …

………………

20180918
(Date): ………………….

Dr Maximo Q. Mejia Jr.
Supervised by: ………………….

MLP
Supervisor’s affiliation: ………………….
Acknowledgements

This paper is the result of my ‘academic adventure’ at WMU, precipitated by a desire to strengthen my shipping credentials after a career move from telecommunications to digital logistics. I would like to thank my professors and classmates for an experience that was both intellectually and socio-economically enlightening. ‘Emerging’ and ‘Frontier’ markets have become real to me as a result of personal connections to sixteen new countries (AZ, CM, CN, ET, GE, GH, GR, KR, LR, PA, PH, SO, TG, TL, VC, VN). I have learned that there are many aspects of shipping which are damaging, exploitative and need urgent attention. I will seek to use my new knowledge and research to make a difference. The WMU Library staff merit special mention for their help. The World Bistro staff did a terrific job on the catering.

I dedicate this paper to my mother Elizabeth Cosgrave, who despite a strong desire and capability was denied the opportunity to pursue formal education beyond grade school. She therefore ensured that her four daughters grew up without limits to their aspirations. With this M.Sc., she now has four graduate and four undergraduate surrogate degrees!

Most importantly, I thank my husband Marc Humblet (merci Cheri!!!) and our daughter Oonagh for their patience and understanding, while I ferried back and forth to Malmo. Although far away, they were always in my thoughts, and with What’s App, frequently on the phone!

2018 was a national election year in Sweden. During the campaign, Malmo was frequently referred to as a ‘dangerous’ city with a ‘migrant problem’. This was not my experience. I found it to be very agreeable with a tremendous cultural offering, an enticing seaside and remarkably clean and uncongested. Any ‘migrants’ I saw or met were productively engaged in work, study or taking care of their families. The world needs to dispel ‘fake news’ and this is an attempt as a correction.
Abstract

Title of Dissertation: Electronic Certificates for Ships, A LOFTy (Legal, Operations, Fraud, Trust) Analysis

Degree: Master of Science

Ship certificate issuance and certificate compliance are core competencies of flag and port States respectively. Guidelines of the International Maritime Organization for implementation of electronic certificates have been available for several years, and a recommended deadline of April 2019 challenges stakeholders to enable ‘the electronic clearance of vessels’ replacing paper certificates with data records.

This paper reviews the legal, operational, fraud and trust aspects of the maritime administration transition to e-government. Change management issues for internal and external stakeholders are covered. Case studies of legislation and implementation are reviewed for best practices that can be adopted by maritime administrators making the digital shift.

In particular, the paper considers an e-Document reference architecture and the “once only principle” (OOP) as tools to support the growing introduction of ‘single windows’ for ship-shore and ship-administration data submissions. An attempt is made to build an "e-maritime maturity index" for leading shipping nations, as a benchmarking tool.

The research confirms that global adoption of electronic ship certificates can improve implementation of IMO instruments. The research may serve as an input document for digital policy and implementing measures by maritime administrations and their contractual relations with recognized organizations. It may also support risk mitigation in implementation projects and the evolution of IMO guidelines.

Keywords: Ship certificates, electronic certificates, maritime digitization, e-government, certificate fraud, Open register, Port State Control,
# Table of Contents

Declaration .................................................................................................................. ii
Acknowledgements ..................................................................................................... iii
Abstract ...................................................................................................................... iv
List of Abbreviations .................................................................................................. viii
1. Introduction .............................................................................................................. 11
2. Ship Certificates Going Electronic ........................................................................ 14
3. Legal Aspects of Electronic Ship Certificates ....................................................... 26
4. Operational Aspects of Electronic Certificates ...................................................... 36
5. The IMO Approach to Electronic Certificates ....................................................... 44
6. Digital Initiatives in Adjacent Sectors .................................................................... 50
7. Fraud & Trust Aspects of Electronic Certificates ................................................. 52
8. The Future Internet of Ships .................................................................................. 59
9. Conclusion and Recommendations ....................................................................... 63
References .................................................................................................................. 65

Appendix 1: Physical Inspection of Ship Certificates & Documents ......................... 76
Appendix 2: Sample Certificate of Registry, Kingdom of the Netherlands ............... 77
Appendix 3: Vessel Registration in Liberia ................................................................. 78
Appendix 4: Ship Certificates Issued Electronically .................................................. 79
Appendix 5: ISA2 Reference Architecture for E-Documents ................................. 81
Appendix 6: MA Press Releases and Maritime Announcements ............................. 82
Appendix 7: Fleet Ownership & Registration, Main Economies, 2017 ...................... 83
Appendix 8 IMO RESOLUTION MSC.428(98) ............................................................... 84
List of Tables

Table 1: Certificates by Issuer with Examples ................................................. 17
Table 2: Timeline of Global Technology & IMO Instruments............................. 23
Table 3: E-Maritime Maturity Indicators of Leading Shipping Countries .......... 42
List of Figures

Figure 1: Shipping Value Chain ................................................................. 14
Figure 2: E-Documents Reference Architecture: E-Document Lifecycle .......... 25
Figure 3: E-Documents Reference Architecture: Legal View ....................... 27
Figure 4: Layne and Lee E-Governance Model .......................................... 37
Figure 5: E-Documents Reference Architecture: Organization View ............. 38
Figure 6: E-Documents Reference Architecture: Semantic View .................. 45
Figure 7: E-Maritime Policy Implementation Stakeholder Feedback .............. 46
Figure 8: Heterogeneous Data Standards in Shipping ............................... 48
Figure 9: Deficiencies in Port State Control Inspections 2016 ...................... 52
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFS 2001</td>
<td>Systematic Work Environment Management</td>
</tr>
<tr>
<td>B</td>
<td>Behaviour</td>
</tr>
<tr>
<td>BIMCO</td>
<td>Baltic and International Maritime Council</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CLASS</td>
<td>Classification Society</td>
</tr>
<tr>
<td>CMDS</td>
<td>Common Maritime Data Structure</td>
</tr>
<tr>
<td>CMP</td>
<td>Country Maritime Profiles</td>
</tr>
<tr>
<td>CO2</td>
<td>Carbon Dioxide</td>
</tr>
<tr>
<td>DG MOVE</td>
<td>Directorate General of Mobility and Transport</td>
</tr>
<tr>
<td>DG TAXUD</td>
<td>Directorate General for Taxation and Customs Union</td>
</tr>
<tr>
<td>DMA</td>
<td>Danish Maritime Authority</td>
</tr>
<tr>
<td>DIGIT</td>
<td>Directorate General of Informatics</td>
</tr>
<tr>
<td>e-/E-</td>
<td>electronic (as a prefix)</td>
</tr>
<tr>
<td>e-IDAS</td>
<td>Electronic Identification and Trust Services</td>
</tr>
<tr>
<td>EPCIS</td>
<td>Electronic Product Code Information Services</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EDIfact</td>
<td>Electronic Data Interchange for Administration, Commerce and Transport</td>
</tr>
<tr>
<td>EMSA</td>
<td>European Maritime Safety Agency</td>
</tr>
<tr>
<td>eMSW</td>
<td>European Maritime Single Window</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Network and Information Security</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUR</td>
<td>EURO currency</td>
</tr>
<tr>
<td>FAL</td>
<td>Facilitation of International Maritime Traffic Convention</td>
</tr>
<tr>
<td>FAL COMM</td>
<td>Facilitation Committee (of the IMO)</td>
</tr>
<tr>
<td>FFE</td>
<td>Fire-fighting equipment</td>
</tr>
<tr>
<td>FI</td>
<td>Future Internet</td>
</tr>
<tr>
<td>FID</td>
<td>Future Internet Enterprise Resource Identifiers</td>
</tr>
<tr>
<td>FloS</td>
<td>Future Internet of Ships</td>
</tr>
<tr>
<td>FlnES</td>
<td>Future Internet Enterprise System</td>
</tr>
<tr>
<td>FlnEr</td>
<td>Future Internet Enterprise Resources</td>
</tr>
<tr>
<td>G2B</td>
<td>Government to Business</td>
</tr>
<tr>
<td>G2C</td>
<td>Government to Citizen</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GISIS</td>
<td>Global Integrated Shipping Information System</td>
</tr>
<tr>
<td>GloMeep</td>
<td>Global Maritime Energy Efficiency Partnerships</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>GMCI</td>
<td>Global Maritime Connectivity Index</td>
</tr>
<tr>
<td>GR</td>
<td>Graphical representation</td>
</tr>
<tr>
<td>gTLD</td>
<td>Generic Top Level Domain name</td>
</tr>
<tr>
<td>IACS</td>
<td>International Association of Classification Societies</td>
</tr>
<tr>
<td>IALA</td>
<td>International Association of Marine Aids to Navigation and Lighthouse Authorities</td>
</tr>
<tr>
<td>IALA MSP 8</td>
<td>Vessel Shore reporting</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>ICT</td>
<td>Information communications technology</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electro-technical Commission</td>
</tr>
<tr>
<td>IHMA</td>
<td>International Harbour Masters’ Association</td>
</tr>
<tr>
<td>IHO</td>
<td>International Hydrographic Organization</td>
</tr>
<tr>
<td>III Code</td>
<td>Code for Implementation of Mandatory IMO Instruments</td>
</tr>
<tr>
<td>ILLC</td>
<td>International Load Line Convention</td>
</tr>
<tr>
<td>ILENT</td>
<td>Netherlands Maritime Administration (flag State &amp; port State)</td>
</tr>
<tr>
<td>IMO</td>
<td>International Maritime Organization</td>
</tr>
<tr>
<td>IPV6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>ISM</td>
<td>International Safety Management</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>ISA2</td>
<td>Interoperability Solutions for Public Administrations</td>
</tr>
<tr>
<td>ITPCO</td>
<td>International Taskforce on Port Call Optimization</td>
</tr>
<tr>
<td>LSA</td>
<td>Life-saving appliances</td>
</tr>
<tr>
<td>M</td>
<td>Memory</td>
</tr>
<tr>
<td>MA</td>
<td>Maritime Administration / Maritime Authority</td>
</tr>
<tr>
<td>MARPOL</td>
<td>International Convention for the Prevention of Pollution from Ships</td>
</tr>
<tr>
<td>MEPC</td>
<td>Marine Environment Protection Committee (of IMO)</td>
</tr>
<tr>
<td>MLC</td>
<td>Maritime Labour Convention</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MT</td>
<td>Metric Tonnes</td>
</tr>
<tr>
<td>MSC</td>
<td>Maritime Safety Committee (of IMO)</td>
</tr>
<tr>
<td>MSW</td>
<td>Maritime Single Window</td>
</tr>
<tr>
<td>N</td>
<td>Networking</td>
</tr>
<tr>
<td>NMSW</td>
<td>National Maritime Single Window</td>
</tr>
<tr>
<td>NVOCC</td>
<td>Non-Vessel Owning Common Carrier</td>
</tr>
<tr>
<td>OCECPR</td>
<td>Office of the Commissioner of Electronic Communications &amp; Postal Regulation (of the Republic of Cyprus)</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OJEU</td>
<td>Official Journal of the EU</td>
</tr>
<tr>
<td>OSI</td>
<td>On-line Services Index</td>
</tr>
</tbody>
</table>
PA3  Pilot Area 3 (in TOOP)
PDF  Portable Document Format
PKI  Public Key Infrastructure
PPR  Public Sector Process Rebuilding
PROTECT  Port Message Design Group
PSC  Port State Control
PSI-II  Directive on the Re-use of Public Sector Information
PSCO  Port State Control Officer
RFD  Reporting Formalities Directive
RO  Recognize Organization
RU  Russian Federation
SMDG  Ship Message Design Group
SOLAS  International Convention for the Safety of Life at Sea
STCW  International Convention on the Standards of Training, Certification and Watchkeeping for Seafarers
TIN  Tracking Identification Number
TOOP  The Once Only Principle
UDEF  Unified Data Exchange Format
UNAP  United Nations Public Administration Network
UNCITRAL  United Nations Commission on International Trade Law
UNCLOS  United Nations Convention of Law of the Sea
UNDESA  United Nations Department of Economic and Social Affairs
UNDPE  United Nations Division for Public Economics
UNEDI  United Nations E-Government Development Index
WCO  World Customs Organization
WG9  Working Group 9 (of IMO FAL COMM)
WMO  World Meteorological Organization
1. Introduction

Global shipping is rapidly heading toward an International Maritime Organization (IMO) recommended deadline of April 2019 for the ‘electronic clearance of vessels’ in which ship electronic certificates (e-certificates) are an enabling factor. In response to demands from stakeholders, and following successful trials with their neighboring maritime administration (MA), in June 2016 the Danish Maritime Authority (DMA) announced a complete transition from paper to electronic format of all statutory ship certificates issued to vessels flying the Danish flag. (DMA, 2016) As a leading maritime state, an active proponent of digitization within the IMO and home to one of the world’s largest container lines, Denmark is among the first flag States to make such a move. Liberia was a fast follower with an announcement October 2016. (Liberian Registry, 2016). While these developments mark a watershed in the digital agenda of global shipping, to-date, fewer than a dozen IMO Member States have officially announced issuance of e-certificates.

The IMO Facilitation Committee (FAL COMM) has provided Member States with guidelines for the use of e-certificates regularly over the past five years. (IMO, 2013). Industry is starting to appreciate that the shift from ‘documents’ to ‘data models’ can enable remote compliance confirmation with limited involvement of the crew. Given that stringent environmental regulations will soon further burden inspection obligations, this would be a good thing. But shipping leadership is notoriously under-invested in digital technologies and more data-centric strategies are urgently needed. (Informa, 2018)

---

1 Guidelines for the Use of Electronic Certificates FAL-5_Circ-39_Rev.2 April 2016: …According to the Standard 3.bis, Public Authorities have to establish systems for the electronic exchange of information by 8 April 2019. A period of no less than 12 months for transition to the mandatory use of the systems shall be provided from the date of the introduction of such systems. A new Recommended Practice encourages the use of the “single window” concept, to enable all the information required by public authorities in connection with the arrival, stay and departure of ships, persons and cargo, to be submitted via a single portal without duplication. https://edocs.imo.org/Final Documents/English/FAL.5-CIRC.39-REV.2 (E).docx
The transition from legacy paper to e-certificates presents challenges and opportunities for a broad range of stakeholders: MAs, port state control officers (PSCO), classification societies (CLASS), shipowners and crew, agents and vetting companies, insurers, financial and legal advisors. All these parties rely on ship certificate issuance, maintenance, endorsement and revision as part of their core business processes. The e-certificate shift coincides with demands from private companies to public authorities for broader data re-use respecting the “once only principle” under which data is shared among related public bodies within the same jurisdiction. In the European Union (EU) there are calls for cross-border re-use of data stored in national databases.

For service providers, e-certificates represent a promising global market for software, hosting and advisory services potentially worth millions of dollars. Industry sources suggest that for a total addressable market of approximately 90,000 ‘SOLAS classed’ vessels (International Convention for the Safety of Life at Sea (SOLAS)), statutory certificates alone represent an annual demand of 3 million certificates (seafarers add another 5 million). But the market has not been properly sized. MA officials struggle to measure certificate volumes due to the lack of genuine key performance indicators. In some cases, shipowners are deemed willing to pay to ‘de-materialize’ certificates given measurable cost savings. The European Commission (EC) estimates that electronic data submission for the 2 million port calls annually in the EU could eliminate 4.6 million hours of shipping sector staff work (European Commission, 2018, p. 1). In addition, secure electronic formats offer robust archiving. The challenge for all stakeholders is to manage the change process to ensure the promised gains are realised and avoidable pitfalls averted.

This study reviews the key concerns of stakeholders, being legality and operational impact. Fraud which has always been a risk with paper documents, and trust which has become more fragile in the digital are both considered in light of technology factors. Part two reviews the history of ship certificates and current industry practice. It
introduces the reader to the concepts of data elements and data models as distinct from documents. Part three reviews legal challenges related to e-certificates, and illustrates soft and hard law in the EU. A multi-country project provides important pointers on legality and a single state initiative illustrates a pragmatic approach. Part four highlights selected operational challenges for MAs to digitize their business processes. An in-depth analysis of e-government and e-certificate indicators ranks shipping nations according to their ‘e-maritime maturity’. The need for greater data harmonization and business process interoperability is discussed. Part five reviews the IMO approach to e-certificates. Part six offers comparable experience with digitization from adjacent industry sectors. Part seven covers topics of fraud and digital trust incorporating cybersecurity. Part eight offers a vision of the future with a conceptualization of the ‘Future Internet of Ships’. Recommendations based on the analysis and findings are summarized in the conclusion. The paper is confined to certificates of registration, periodic surveys, and others related to Code for Implementation of Mandatory IMO Instruments (revised) (III Code). (IMO, 2017), excluding log-books and seafarer certificates. The term e-certificate means electronic ship certificates unless otherwise qualified.

Research methods used in this paper reflect the global scope and evolving technological landscape related to e-certificates. Desk and field research have provided a descriptive overview and analytical insights. Data was sourced from multiple formats including journal articles, books, web-sites and stakeholder body publications. The contemporary nature of the topic dictated a literature review primarily focused on materials published since 2007. Qualitative analysis of source documents was complemented by findings from extensive field research conducted through face to face meetings with industry practitioners. The author has monitored multiple IMO meetings and extensively reviewed IMO documents. Case studies of implementation practices in a few countries provided understanding of key legal and operational issues. Identities from field study activities have been masked and general conclusions have been drawn.
2. Ship Certificates Going Electronic

This section reviews the history of, and different types of ship certificates. It introduces the reader to the concepts of data elements and data models as distinct from documents. The timeline of digital technology adoption in society at large is juxtaposed with maritime certification instruments to illustrate the digitization lag. In closing, the EU standard for e-documents as a frame of reference for e-certificates will be introduced.

Figure 1 provides a visualization of the inter-dependent elements in the shipping value chain. Ship certificates fall within the ‘Regulation’ layer. (Ramboll & CORE, 2017, p. 9) Whether a ship certificate is paper or electronic will impact the business models, competencies/processes in the other parts of the value chain given that the technologies and infrastructure needed to use either format differs. Enforcement and insurance represents the public and private sector spheres that rely on the certificate as evidence. While this paper does not follow this construct to the letter, most of these segments will be considered, to the exclusion of insurance.

Figure 1: Shipping Value Chain

Source: Ramboll & CORE
Ship certificates, be they paper, portable document format (PDF) or purely electronic are essential documents testifying the seaworthiness of vessels, allowing them to trade. Ship certificate issuance and cancellation, endorsement, acceptance, inspection and control are core competencies of IMO convention parties and/or contracting governments, flag States and port States respectively. Statutory certificate issuance is provided by the MA or their sub-contracting service provider, typically CLASS, in which case they are referred to as Recognized Organizations (ROs). A key stage of the vessel inspection process by a third country PSCO is verification that all certificates and documents of the vessel are in good order.

Historically, certificates have been issued on paper, carried physically on board the vessel and furnished by the crew to the PSCO upon request (see photographs in Appendix 1). Certificate deficiencies may contribute to justification for a ship detention. In 2018, this practice of ‘handing over of paper documents’ is largely still in place for the vast majority of PSCO inspections, ignoring repeated calls to action to shift to digital, including IMO guidelines from 2014. (IMO, 2014) Despite the wide availability of smartphones which now represent 57% of the 5 billion mobile phones worldwide (GSM Association, 2018), smartphone based tools to support PSCOs are rare, with the Indian Ocean MOU being one the first to offer such. (Indian Ocean MOU, 2015) Barriers to technology adoption are aptly summarized by FAL COMM: “…countries still maintain requirements which run contrary to these facilitation efforts, because of historical precedents, commercial inertia, difficulty in adjusting the methods of their control bodies, or ignorance of solutions that have been developed elsewhere.” (IMO, 2013, p. 2)

The practice of registration certificates (certificates of ownership) serving to authenticate ownership of vessels emerged in the XVII century. In the Anglo-Saxon world, vessel registries started with the United Kingdom Shipping and Navigation Act of 1786. Vessel details were provided by shipowners to customs officers in their home port, with each ‘certificate of registry’ numbered and entered into a registration book being the Port Register. Copies were sent to the central registry referred to as the
‘Board of Trade’. (Watt, 2014, p. 9). Much as today, certificates contained details of the vessel, ownership, original master and reason and date of closure of the registry. Subsequent transactions, including mortgages and change of ownership were recorded on ‘port certificates’. Historical records confirm that a similar approach was used in the British Colonies including Canada as well as the Baltic, Italian and Spanish shipping regions. (MUN, 2018).

Certificates of ownership remain the first document of public record for a ship. Depending on the practices of the flag State in question, upon registration a shipowner receives statutory certificates which are proof of ownership, allocated to the vessel making it subject to that jurisdiction with respect to safety regulations, security, crewing, etc. There are two initial documents: the Certificate of Registry which is evidence of ownership and nationality of the ship and includes ship particulars (name of the ship, the date of construction, the gross and net tons, length over all, and length between perpendiculars, breadth, draught, registry and flag, call sign or code number, names of owners and master) and the transcript of Registry, a publicly accessible document which includes the ownership details and a history of any mortgages or liens against the vessel. Appendix 2 provides a sample Certificate of Ownership from the Kingdom of the Netherlands. When the vessel is sold, the registry issues a Certificate of Deletion. (Sullivan, 1999, p. 85) With the Certificate of Registry, the ship is granted the right to ‘fly the flag’ of the country, which affords diplomatic, consular and naval protections and services. The flag also confers rights related to the country’s territorial waters, and the implications of the rules of war. (Watt, 2014, p. 7) Appendix 3 is a graphical representation of the ship registration processes as a flowchart from the Liberian Registry, which is indicative of general industry practice.

Under the United Nations Convention on Law of the Sea (UNCLOS) Art.217 (Enforcement by flag states), flag States are obliged to ensure that all vessels registered under their flag, comply with international rules and standards, laws and regulations. (International Tribunal of the Law of the Sea, 1982, p. 216) In this context, the MA
issues various certificates as documentary proof of compliance with relevant national laws and IMO instruments which the shipowner, operator and master must have available ‘onboard’. The list of certificates and documents required to be carried on board ships as at 2017 is distributed over four separate IMO publications: FAL.2/ Circ.131/ Corr.1; MEPC.1/ Circ.873/ Corr.1; MSC.1/ Circ.1586/ Corr.1 and LEG.2/ Circ.3/ Corr.1. These various other certificates are issued either by ROs acting on behalf of MAIs, or by MA staff, acting as surveyors of their own national fleet. The same staff can also act as inspectors of third country vessels for port State, to confirm compliance. Table 1 summarizes the main groups of certificates (RINA, 2015)

<table>
<thead>
<tr>
<th>GROUP</th>
<th>ISSUED BY</th>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship Certificates</td>
<td>Flag State / RO</td>
<td>Load Line, Document of Compliance, International Safety Management</td>
</tr>
<tr>
<td>Class Certificates</td>
<td>Class</td>
<td>Hull, Engine, Operation</td>
</tr>
<tr>
<td>Equipment Certificates</td>
<td>Flag State/ RO</td>
<td>Voyage Data Recorder</td>
</tr>
<tr>
<td>Ship Documentation</td>
<td>Owner, Builder</td>
<td>Stability booklet, Safety plan, Mandatory operational routines e.g. SOPEP, SMPEP etc.</td>
</tr>
<tr>
<td>Log books, Records</td>
<td>Crew / Master</td>
<td>Deck, Engine, Drills</td>
</tr>
<tr>
<td>Crew Certificates</td>
<td>Other Authorities</td>
<td>Master, Officers and Ratings, Medical</td>
</tr>
<tr>
<td>Insurance</td>
<td>Insurance Companies</td>
<td>Liability, Pollution</td>
</tr>
<tr>
<td>Cargo and Holds</td>
<td>Shipper, Operator</td>
<td>Cargo information, Dangerous Goods Manifest, Gas free certificate</td>
</tr>
</tbody>
</table>

Source: RINA

Depending on the size & type of the vessel, the master will have several dozen certificates, (varying in length from one to several pages each), to document compliance. This includes statutory certificates for various conventions *inter alia* SOLAS, International Convention for the Prevention of Pollution from Ships (MARPOL), International Load Line Convention (ILLC), Maritime Labour Convention (MLC), as well as all supporting certificates such as CLASS, fire-fighting
equipment (FFE), life-saving appliances (LSA) and other various equipment. (DMA, 2016) For example, the DMA, issues more than 60 different types of statutory certificates covering all categories of vessels: cargo ship, passenger ship, fishing vessels and other (ie barge, offshore), all electronically. Appendix 4 is an indicative list of certificates which may be issued by a flag State administration.

To paraphrase Maher, ship certificates are credentials that allow the holder to exercise certain rights and privileges, being those provided to registered ships under the relevant flag (USA Patent No. 6,125,349, 2000). They are documents which represent certified assertions about the ship. These assertions are certified by the flag State administration and/or their RO. Typically the assertions pertain to a vessel possessing certain characteristics or sufficient equipment, systems, standard operating procedures or processes in practice so as to satisfy the criteria of the relevant regulatory requirements. The assertions can be presented in the form of prose sentences, but much of the information is factual data. Such data has been defined by the ISO/IEC 2382-1 standard as “A re-interpretable representation of information in a formalized manner suitable for communication, interpretation or processing.” (IMO, 2013, p. 68) Each IMO instrument which generates certification provides sample templates as a minimum data capture, on which Member States can and do model their documents. Given the lack of official standards, MAs are not prevented from adding their own requirements.

The state event which validates these assertions is the ship inspection or ‘survey’. Whether the certificate is paper or electronic, the data is entered into the relevant field of the template (becoming a data element) in order to complete the form (a data record). Historically, free text, (often handwritten) was added to the certificate by the surveyor. The IMO refers to ISO 9735 V4. Part 1 for a definition of data elements being “A unit of Data described in a data element specification.” (IMO, 2013, p. 68) The form completion is testified by the signature of the authorized person, being a nominated signatory of the MA or their RO. Hand-written signatures are still used.
extensively. While they can make paper documents auditable, (being verifiable post-hoc), the time and energy necessary to trace handwritten signatories, compared to a certified digital signature, favor the latter. E-certificate data elements are protected from tampering by means of a ‘digital signature’ which replaces the handwritten signature. The digital signature is a cryptographic mechanism that ensures the data is unique and only accessible to third parties through the use of public information being the public key infrastructure.

The certificate inspection process for PSC is closely defined and has been recently updated, as detailed below. Although e-certificates are clearly mentioned in these instructions, it is interesting to note that direct submission of data by the shipowner/operator to the public authorities in anticipation of the port call is omitted:

2.2.3 On boarding and introduction to the master or the responsible ship's officer, the PSCO should examine the ship's relevant certificates and documents required by the relevant conventions, as listed in appendix 12 part A.

PSCOs should note the following:

.1 certificates may be in hard copy or electronic form;
.2 where the ship relies upon electronic certificates:
  .1 the certificates and website used to access them should conform with the Guidelines for the use of electronic certificates (FAL.5/Circ.39/Rev.2 and Corr.1);
  .2 specific verification instructions are to be available on the ship; and
  .3 viewing such certificates on a computer is considered as meeting the requirement that certificates be "on board";
.3 when examining 1969 International Tonnage Certificates, the PSCO should be guided by appendix 10; and
.4 when examining certificates or documentary evidence of seafarers issued in accordance with STCW 1978, the PSCO should be guided by appendix 11; the list of certificates or documentary evidence required under STCW 1978 is also found in table B-I/2 of the STCW Code. (IMO, 2018, pp. Annex 1, p.10)
Paper certificates presented to PSCOs for verification during inspection can create challenges to comprehension. In contrast, e-certificates as ‘digital credentials’ and the data elements therein can be presented for inspection remotely for interpretation and validation to the computer systems of the relevant authorities. In the transition away from paper, the ‘certificate’ is in effect replaced by an electronic data record of data elements, presented in a data model defined by the terms of the certificate template, protected by a digital signature that ensures data veracity. Transmission of the certificate(s) can be either by the shipowner or his authorized delegate, be it crew or ship management company.

During various field visits conducted since early 2017, the author found that in countries which pride themselves on fully digital e-government services in health, education or taxation, the MA is seemingly locked in a pre-digital time-warp, as illustrated by the following anecdotes. In an EU country, a senior MA official confirmed regional personnel retained thousands of survey records used as the basis of certification, in paper files in filing cabinets with no back-up. His primary data security concern was not a cyber-attack but rather the risk of fire. A leading RO senior staff member confirmed that large quantities of paper certificates were regularly airmailed or couriered to their clients in the Far East. In one leading flag State, senior staff regularly downloaded PDFs received from ROs, printed them onto paper and stored them in binders in the office presumably for want of a convenient electronic records management system and/or under-developed e-skills. Finally, a senior partner in a leading maritime law practice, was puzzled by the need to convert to digital formats, since the veracity of certificates was delegated to ship management companies with no apparent need by legal counsel to validate their existence, neither physically nor electronically. Such due diligence methods would be quite unheard of in other industry domains. Clearly this user community has business practices that pre-date the internet era.
The IMO is long on generic descriptions and short on a programme to systematically dismantle barriers to the adoption of e-certificates. Factual data on the actual volume of certificates issued and specific blocking factors are not readily available. The e-certificate definitions as per the guidelines are as follows:

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

2. E-certificate means a certificate issued in an electronic format; accessible for viewing through or via a website or, a ship’s computer, or a printed version of such certificate; or other digital media and used to create a printed version. Printed version of e-certificate means a paper certificate print-out produced from the e-certificate;

3. E-signature means data in electronic form which is attached to or logically associated with other electronic data to serve as a method of authentication of the issuer and contents of the electronic data;

4. Unique tracking number means a string of numbers, letters, or symbols used as an identifier to distinguish an e-certificate issued by an Administration or its representative from any other e-certificate issued by the same Administration or its representative; (NB: there is no agreed global standard for the tracking numbers) and

5. Verification means a reliable, secure, and continuously available process to confirm the authenticity and validity of an e-certificate using the unique tracking number on board the ship with the source issued by the Administration or its representative that issued the certificate.

(IMO, 2014, pp. Annex 1-2)

All of this is important because the scope of IMO related ship certificate issuance is growing steadily. According to a report by the Russian Federation (RU) submitted to the IMO, their analysis of more than fifty IMO statutory instruments confirmed that the number of mandatory certificates and documents has grown from 25 entries in
1990 to 60 in 2004, and more than 100 in 2017. (Russian Federation, 2017) The IMO Global Integrated Shipping Information System (GISIS) Surveys and Certification module lists 62 certificates. (IMO, 2018). RU expressed concern that the transition to e-certificates will not alleviate this expansion trend, but rather may exacerbate it. Coincident with the expansion of certificate scope, attempts to harmonize or standardize terminology and syntax in a globally uniform way to be used in certificate documents and more broadly in Maritime Single Windows (MSW) remains unfinished (more on this below).

In shipping, documentary evidence, rather than data, remains the *modus operandi* to prove statutory compliance. Ships’ crew show a PSCO a piece of paper or an electronic file of a document, they do not ‘share data’. This is the very heart of the administrative burden, and it reflects the IMO reporting obligations legacy. Staying with the same time period selected by RU, a benchmark to digital technology shows clearly the backwardness of paper ship certificates. From the perspective of digital media research fellow Cotton, during the 1990-2017 period, decisive trends have been massive increases in computing power, (also available on diverse mobile devices), massive content digitalization, and ever-increasing on-line connectivity coverage and capacity. These three global societal shifts have until now, left ship certificates largely unchanged. Breakthroughs yet to be fully exploited include: artificial intelligence including narrative software agents, ‘internet of everything’ telemetry and telematics (satellites, remote sensing, drones etc.), robotics and virtual robotics. (Cotton, 2018). Table 2 provides a timeline, tracking major global technology breakthroughs alongside the issuance of IMO instruments. It clearly illustrates that although multiple enabling technologies have been available to the shipping industry for some fifty years and many pre-date SOLAS, they have been pretty much ignored by IMO stakeholders, notably the MAs and their ROs.
### Table 2: Global Technology & IMO Instrument Timeline

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TECHNOLOGY MILESTONES</th>
<th>SHIPPING REGULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>Cognitive Computing / IBM &quot;Watson&quot;</td>
<td>DMA announces all ship e-certificates Liberia /ClassNK announce e-certificates</td>
</tr>
<tr>
<td>2012</td>
<td>Oculus Rift, Virtual Reality</td>
<td>Cape Town Agreement 2012 (Fishing Vessel safety)</td>
</tr>
<tr>
<td>2004</td>
<td>Facebook/ Social Media 2004 LENOVO (China) buys IBM PC 2004</td>
<td>Ballast Water Management Convention 2004</td>
</tr>
<tr>
<td>1999</td>
<td>1st 3G mobile license in Finland Mobile phones affordable in OECD</td>
<td></td>
</tr>
<tr>
<td>1994</td>
<td>Bluetooth Wireless standard E-commerce websites start Play Station in Japan</td>
<td>International Safety Management (ISM) Code</td>
</tr>
<tr>
<td>1993</td>
<td>Adobe Acrobat 1.0 PDF format</td>
<td>UK Merchant Shipping (Registration of Ships) Regulations 1993 / Tokyo MOU 1993/ CSC Amendments 1993 / SFV Protocol 1993</td>
</tr>
</tbody>
</table>

Source: B.Cosgrave compiled from various sources incl. in references
Table 2 (cont’d): Global Technology & IMO Instrument Timeline

<table>
<thead>
<tr>
<th>YEAR</th>
<th>TECHNOLOGY MILESTONES</th>
<th>SHIPPING REGULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1990 - 91</td>
<td>WWW/ Tim Berners Lee 1990</td>
<td>US Oil Pollution Act 1990</td>
</tr>
<tr>
<td></td>
<td>Digital Audio Broadcasting 1990</td>
<td>PAL Protocol 1990</td>
</tr>
<tr>
<td></td>
<td>LINUX O/S 1991</td>
<td>OPRC Convention 1990</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SALVAGE Convention 1989</td>
</tr>
<tr>
<td>1987</td>
<td>Nordic Mobile Telephony 900 in DK</td>
<td></td>
</tr>
<tr>
<td>1984 - 86</td>
<td>APPLE Mac PC 1984</td>
<td>UN Ship Registration Convention 1986</td>
</tr>
<tr>
<td>IBM Personal Computer 1981</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1978</td>
<td>Internet 1975</td>
<td>STWC 1978 (EiF April 1984)</td>
</tr>
<tr>
<td></td>
<td>Digital Camera 1975</td>
<td>SOLAS Protocol 1978</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MARPOL Convention 1978</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR Convention 1979</td>
</tr>
<tr>
<td></td>
<td>Graphic User Interface (GUI) 1973</td>
<td>SOLAS Safety of Life at Sea Convention 1974 (EiF</td>
</tr>
<tr>
<td>1972 - 73</td>
<td>Mobile Phone 1973</td>
<td>Space STP Protocol 1973</td>
</tr>
<tr>
<td></td>
<td>Graphic User Interface (GUI) 1973</td>
<td>Intervention Protocol 1973</td>
</tr>
<tr>
<td></td>
<td>INTEL 4004 1972</td>
<td>MARPOL Convention 1973</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collision Regulations (COLREG) 1972</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSC Convention 1972</td>
</tr>
<tr>
<td></td>
<td></td>
<td>London Convention 1972</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nuclear Convention 1971</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UK Merchant Shipping Act 1970</td>
</tr>
<tr>
<td></td>
<td>Electronic Data Interchange 1968</td>
<td>Intervention Convention 1969</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLC Convention 1969</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Load Lines Convention 1966</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Facilitation Convention 1965</td>
</tr>
</tbody>
</table>

Source: B.Cosgrave compiled from various sources incl. in bibliography

Given a growing reliance on certification compliance, global shipping needs an e-certificate approach which is holistic, covering legal, organization, semantic and technical aspects. Sadly neither the IMO, nor any other shipping standardization body has provided one, nor recommended any existing model. Research for this paper identified the "e-Documents Reference Architecture" from the Interoperability Solutions for Public Administrations (ISA2) program of EC Directorate General of
Informatics (EC DG DIGIT) as a best practice model. (EC, 2018) The ISA2 frameworks lend themselves to the analysis of e-certificates and will be referred to hereafter. The life-cycle of e-certificates can follow the flow illustrated in Figure 2. (JoinUp, 2016) A graphical depiction of the full ISA2 reference architecture is provided in Appendix 5.

**Figure 2 : E-Documents Reference Architecture: E-Document Lifecycle**

Source: European Commission ISA2

This section has provided an introduction to ship certificates and placed the ongoing digital transition in perspective. E-certificate creation in shipping is currently heterogeneous, including disparate formats from multiple actors with only the bare minimum of standards universally agreed. Methodologies for e-certificate exchange, preservation and deletion, are left to MAs and ROs to be managed independently. In the 21st century, statutory certificates predominately issued on paper or in PDF format (itself a 25 year old technology) are sent across the globe, replicated and/or copied for sharing between parties. In such a format, data elements contained therein, cannot be extracted independently of the entire document, resulting in highly cumbersome validation. The following sections will delve deeper into the legal, operational and fraud and trust aspects of electronic certificates.
3. Legal Aspects of Electronic Ship Certificates

This section reviews the legal aspects of electronic ship certificates being principally public administrative law and legislation governing evidentiary documents in electronic form. MAs in leading shipping nations will be assessed for their ‘e-maritime maturity’. An in-depth look at multi-country and single state implementations will cover pending ‘hard law’ instruments. These initiatives reflect ‘first movers’ frustrated with the lack of progress in the protracted IMO consensus model.

Legislation enabling MAs to operate digitally is typically non-maritime specific, stemming from national policy to adapt administrative law to digital methods and instruments, commonly referred to as ‘e-government’. Since the start of this century, governments globally have seized the opportunity to improve service quality and efficiency through exploitation of on-line services. The e-government trend gained momentum in the early 2000’s as a result of a public administration shift from paper-based to digital procedures following the broad adoption of “e-commerce” in the private sector. E-government is now globally well established. As a result, the academic research and policy debate have moved beyond administrative law amendments to current topics of inter-operability, higher-order sophisticated services and legal questions pertaining to admissibility of social media as evidence in trials (Westlaw, 2017). An in-depth analysis of the full range of e-government implementing acts, the law of electronic transactions and the law of evidence is beyond the scope of this paper. The rest of this section is focused on e-government legislative changes as they relate specifically to e-certificate deployment by MAs.

Under European law, the state of the art for e-document solutions (of which e-certificates are a specific case) starts with the public policy principles of ‘once only’ and ‘digital by default’. Best practice indicates that e-maritime legislation and regulations should be elaborated respecting these two principles to the greatest extent possible. Figure 3 illustrates the scope of legal matters to be considered for e-document
issuance in a government context as per the EC ISA2 model. (JoinUp, 2016) The legal framework encompasses requirements and constraints.

**Figure 3: E-Documents Reference Architecture: Legal View**

Legal requirements include administrative procedure legislation and e-government legislation, which as noted are widely adopted since the early 2000s. The former, is typically a legacy legislative instrument and the latter a public law instrument to reflect advances in private law. Journal articles treating e-government legal questions are rather dated. An authoritative study from 2001 by Eifert et al. was commissioned by the Netherlands in anticipation of their administrative law revision. (Eifert, Girot, Groothuis, & Prins, 2001) It focused on national public administration legislation to permit electronic services, typically as part of pan-agency, pan-department programs. The study found implementation varied based on government openness to innovation, country regulatory traditions and the digital legacy of technology integrations into government processes. Key questions included defining equivalence for terminology, such as ‘written’ and ‘signature’ from paper for electronic documents.

E-government first movers included the United States (US), United Kingdom (UK), Australia and Canada. Of these countries, only the UK has an e-certificate initiative underway. The US started with e-government in 1993 albeit in a non-coordinated way with statutory regulations adapted at the specific organization level. The US does not yet issue ship e-certificates. Leading EU countries included Finland with the 2000 Act
on Electronic Services in the Administration and the Netherlands with amendments to
the Dutch General Administrative Law Act as from 2001. Finland is participating in
the ‘The Once Only Principle’ project (TOOP) (details below). German federal law
allowed e-government to launch initially without a change to the public administration
procedure law (Art. 10 VwVfG), albeit it was soon discovered that thousands of
specific regulations stipulated written documents, hand-written signatures, or physical
presence and had to be adapted accordingly. Norway implemented legislation in 2001
to facilitate electronic documents under both public and private law. (Eifert, Girot,
Groothuis, & Prins, 2001, pp. 59-60) Both Germany and Norway are now issuing ship
e-certificates. As for the Dutch, their national fleet of 1,600 vessels operate with paper
certificates and plans from 2016 for e-certificates are yet to be put into effect. This
situation is somewhat incongruous with the Netherlands having endorsed the initial
IMO e-certificate proposal in 2005, being home to the largest port in Europe in
Rotterdam and the Paris MOU in the Hague and the Dutch government as e-
government forerunner since 2001.2

Legal constraints for e-documents include personal data protection and archiving
legislation. An example of the former is the EU General Data Protection Regulation
2016/679 (GDPR) regulating the processing of any personal data relating
to individuals by an individual, a company or an organization in the EU. (EC, 2018)
The GDPR has set a world standard obliging personal data-holders to protect and
secure it. (This is relevant to crew e-certificates). The EU Implementing Rules for
Document Management provide a scope echoing the e-document lifecycle in Figure 2
above. Archives are defined as “… current records, intermediate records and definitive
archives…” For effective implementation, archiving requires good document
management organization, adequate staff training and modern electronic document
management and archiving systems. (EC, 2009).

2 2003 ‘Modernizing Government's program’, the ICT and Administrative Burden (ICTAL) program,
the 2002, ‘Better Government for Citizens and Businesses’(B4 program) and since 2001 the Ministry
of Interior and Kingdom Relations ICT Unit (ICTU), in charge of coordinating e-government
development. (EC, 2015)
Two of the most thorny legal issues related to ship e-certificates, being signature validity and issuer validity, have been treated comprehensively in EU directives. 1997 saw the publication of the “European Initiative in Electronic Commerce” to ensure security and trust in electronic communication. A European framework for digital signatures and encryption was followed by the 1999/93/EC Directive on a Community Framework on Digital Signatures. (OJEU, 2000) Directive 1999/93/EC was repealed with the entry into force 1 July 2016, of the Electronic Identification and Trust Services (eIDAS) Regulation. eIDAS is important and useful since it has harmonized a series of digital signatures, seals, time stamps, registered delivery, and website authentications across national borders, eliminating many areas of confusion. (Notably, IMO e-certificate discussions were blocked by questions over signatures, seals, and stamps for years.) As a result, EU e-signatures have legal equivalence to physical counterparts. E-IDAS generated new trust centers to ensure that online signatures and certificates are authentic (Liptak, 2016). Various national legislative instruments to support e-government conversion have been implemented in EU Member States.³

E-certificates may be implemented with a soft law or hard law approach. Typically countries start with soft law and if that fails to generate the desired behavior from stakeholders, then hard law will follow. Such has been the case at EU level with the soft law instrument, the Reporting Formalities Directive 2010/65/EU (RFD). The RFD applied to all ships calling at 1,200 ports in 23 Maritime EU Member States. The goal to establish a harmonized national maritime single window (NMSW) for facilitation in each country was consistent with the ‘Digital Agenda’, a high-level EU policy

³ Spain: Law 11/2007 on Citizens' Electronic Access to Public Services (LAECSP)
Law 39/2015 the Common Administrative Procedure of the Public Administrations. (Kingdom of Spain, 2015).
Neither the Bulgarian MA nor Spanish MA issue ship e-certificates.
promoting e-government. RFD was supported by significant funding (€37M from 2012-15), engagement by most MAs and industry stakeholders and had sophisticated program management. However it became a case study of what can go wrong with soft law. By the 2015 deadline, only two countries were ready, four others almost ready and remainder not ready at all. RFD ultimately failed due to unclear directive text; various legal frameworks; disparate digital systems, (lack of) standards and (too much) legacy; all compounded by MAs caution and lack of coordination (even within national jurisdictions). (PWC Panteia, 2017)

The RFD was subjected to a legislative ‘fitness test’ 2016-17 followed by a proposal to repeal the soft law and implement hard law with the binding ‘eMSW Regulation’ (Regulation establishing a European Maritime Single Window environment). (EC, 2018). The new eMSW regulation has its legal basis in Article 100 (2), of the Treaty of Rome. Although it does not formally mandate e-certificates, eMSW will require maritime transport operators to submit data via a common interface software, complying with a comprehensive data set, the scope of which will include all EU relevant reporting obligations and international legal acts (read IMO instruments) related to a port call. Although not impossible, it would be completely impractical for the data gleaned from various ship certificates to be transposed from paper certificates manually to the eMSW. Hence this new regulation will provide a de facto shift to e-certificate adoption by at least all ships calling at EU ports. (EC, 2018, p. 10)

Despite the frustrations of the RFD, it is encouraging to see that the highly topical EU funded TOOP project of cross-border data-sharing between government agencies, includes a use case for ship and seafarer certificate data exchange between eight countries\(^4\), referred to as the Maritime Pilot Area 3 (PA3). (Graux, 2017) PA3 addresses a smaller scope of data between fewer countries than the initial RFD failure. It includes MA national database interconnection via systems integration on a platform

\[^4\] Bulgaria, Denmark, Estonia, Finland, Italy, Greece, Latvia, Lithuania, Norway
for on-line ship or crew certificates issuance by flag States, and data-sharing with relevant parties: port authorities, police & border guards etc. (Dimitriou, 2018)

TOOP is particularly relevant to this study, given its in-depth analysis of legal challenges from the perspective of participating MAs. General legal principles covered included: data protection, data sovereignty, purpose limitation, liability, and their impact on the application of the once-only principle at the cross-border level and finally subsidiarity (irrelevant outside the EU). A systematic analysis of source documents included: EU Charter of Fundamental Rights, General Data Protection Regulation, Single Digital Gateway Regulation, e-IDAS Regulation, PSI-II Directive, Services Directive and the e-Commerce Directive. The PA3 legal analysis referred to the IMO at the global level, the EU at the regional level and respective national legislations. From the IMO, emphasis was placed on SOLAS 1974, STCW 1978 and Facilitation of International Maritime Traffic Convention 1965. (AFS 2001 and MARPOL 1973 conventions were outside PA3 scope.) The EU covered directives RFD 2010/65/EU, Safe Sea Net 2002/59/EC and the EU Decision 70/2008/EC for a paperless environment for customs and trade. In its conclusion, TOOP highlighted the persistent ambiguity in IMO around ‘original form’ that perpetuates the PDF format as a way to satisfy the ‘very non-digital age’ IMO obligation to have documents available onboard. (Graux, 2017, p. 46)

The comprehensive scope of legal principles and requirements reviewed by TOOP determined the following compliance needs for the maritime pilot. These findings highlight the advantages of e-certificates and are important learnings for MAs preparing to issue them.
• **Good Administration**: nothing maritime specific, the existing practice of captain’s presentation of paper certificates undergoes a change to a digital mode, with added logging and audit controls, which are an improved level of transparency and allow for post hoc control.

• **Privacy, data protection and confidentiality**: crew certificate data needs to comply with relevant data protection laws. Data processing for certificates is based on legal necessity clearly indicated in IMO, EU and national laws. Once again, e-certificates provide improvements over paper with respect to traceability of data access, and allows for more control since when necessary, data access rights can be subjected to appropriate levels of authorization, which is considered a bonus for personal medical data.

• **Lawfulness and compliance**: The legal basis is IMO Conventions, EU Directives and national laws; for the PA3 pilot, electronic access to certificate data is subject to permission of the captain. However this can be substituted by the MA or the shipowner or their authorized party.

• **Control**: in PA3, the captain controls authorization of certificate data transfer to authorities, acting digitally rather than physically; TOOP suggests that if certificates are not stored locally on the vessel, authorized access of the captain can be built on national identification tools in compliance with, for example the e-IDAS regulation, but this is not obligatory. The risk of abuse, with captains accessing certificates not of the vessel of which they are master, is mentioned, as a consideration for necessary identity access.

• **Value, validity and evidence**: Certificate value and validity are determined according to IMO Conventions and EU Directives. Crew certificates are validated by their issuer through unique identification numbers.

• **Security**: The evidence exchange mechanism shift (from paper-based to digital processes), requires competent authorities and any other party with whom they are engaged, to apply ‘appropriate technical and organizational measures’ relevant to the risk. PA3 suggests pseudonymization and encryption of personal data together with systems which ensure confidentiality, disaster recovery and business continuity which are standard operating procedures for any well-functioning information technology department or service provider. It also suggests reliance on high-level security requirements in IMO Conventions and EU Directives. (Graux, 2017, pp. 48-51)
In contrast, FAL COMM e-certificate guidelines are highly prescriptive with respect to the instrument itself and less stringent on process and verification. MAs are instructed their e-certificates should have specific features such as validity and consistency of format and content with the relevant IMO instrument; be tamperproof (protection from editing, modification, revisions); have a unique tracking number, a printable and visible symbol that confirms the source of issuance and verification websites; be controllable via the safety management systems as per Sec. 11 of the ISM Code; e-signatures to comply with authentication standards adopted by the Administration. In the event the IMO becomes more ambitious, the TOOP framework may be relevant as a model for comparable regional initiatives.

The legal implications of the TOOP multi-country initiative can be compared with a single country implementation, that of Denmark. On 20 June 2016, the DMA announced that as from 24 June 2016 the Kingdom of Denmark would issue all ship certificates covering SOLAS, MARPOL and “other relevant conventions” requirements electronically, in alignment with the IMO Guidelines as per FAL.5/Circ.39. DMA took the precautionary measure to ensure that the e-certificates retained the ‘look’ of paper documents even if it was impossible to retain the ‘feel’. Danish e-certificates bear the coats of arms and a facsimile signature of the authorized signatory, being the inspector, together with the ‘stamp’ of the DMA when viewed on screen or a printed facsimile (the certificate is uniquely electronic). This was done to appease the longstanding ‘signature, stamps and seals’ debate which had blocked FAL COMM meetings for about a decade. Verification is available using the certificate unique tracking identification number (TIN) via the webpage www.dma.dk, accessible by public internet with personal computers or internet enabled mobile (smart)phones, or alternatively by email or by direct telephone. DMA e-certificates are tamperproof due to encryption and digital file signature protection.
DMA instructions to Danish flagged vessel owners, operators and masters, allow that e-certificates be presented either electronically on a computer screen or in a printed colour version, and each vessel is invited to retain the announcement letter to share with PSCOs. (John, 2016) The obvious question is how did the Danes make this happen before any other IMO member state? Is there a particular legal framework that allowed this ‘giant leap forward’? The simple answer is no. The Danes, tired with the decade-long IMO timeline, with characteristic pragmatism ran a pilot trial to make sure that it could work, and then deployed. Prior to the launch, the DMA business processes resembled the early twentieth century. Paper certificates were printed, stamped, signed and sent around the world to wherever the vessel that needed the updated document happened to be. A pilot project started in 2013 with one passenger ferry company operating between Denmark and Norway. The outcome was positive, with a confirmation that e-certificates could replace paper versions. The DMA did not abandon the IMO process, rather they acted on IMO guidelines, as so far, too few top shipping nations have done. Throughout the transition, DMA enjoyed very strong support from Danish Shipowners, the trade association, whose members were eager for the benefits of faster certificate handling, real-time updates to ship management systems and company databases, increased security and more reliable authenticity.

The legal status of ship e-certificates is a national question for flag States and port States. From the scholarly literature, it is clear that at least all OECD countries have made the shift from paper based administrative law to digital administrative law. For developing countries, the UN E-Government Survey has been tracking progress periodically since 2008. Complete online interaction is now globally possible, supported by model legislation, extensive implementation models, project management methodologies, sector specific or geographic benchmarking mechanisms, all available in the public domain. Effectively any MA can offer all its services on-line with legal certainty by referencing international and national legal instruments.

5 Denmark, Germany, India, Korea, Liberia, Norway, Panama, Singapore
In summary, the legal considerations of e-certificates include national administrative law enabled for on-line service delivery and e-government. Research show that this has been the regular mode of operation for governments globally for at least the past decade, (if not two), including Emerging and Frontier Market (developing) countries. Various legal principles apply to ship certificates when they go electronic, such as data protection, data sovereignty, purpose limitation, and liability, but countries that have made the transition or are underway with trials have found these to be manageable. IMO Member States have at their disposal a plethora of guidelines and draft text to support changes to regulations and legislation if required.

Legal challenges for MAs in the areas of national law and public policy are driven by their status as a member of the relevant international organization, being the IMO, their ratification of international conventions, and the relative importance of the shipping sector to their national economy. (Ramboll & CORE, 2017, p. 16) E-certificates apply in many domains often with responsibility shared between the MA and other departments such as national security, transport, labour, environment, justice etc. E-government legislation and regulations covering the legality of electronic communications from legal persons to administrations and vice versa are now well entrenched. While ubiquitous ‘always-on’ connectivity has generated ‘digital trust’ challenges, corrective measures such as GDPR and eIDAS are available. Given the shared responsibility, a review of country e-government indicators together with maritime specific metrics can be combined to indicate ‘e-maritime maturity’ as a measure of preparedness for ship e-certificates issuance. This will be elaborated in the next section.
4. **Operational Aspects of Electronic Certificates**

This section examines selected operational aspects of e-certificate implementation as a comprehensive treatment is beyond the limits of this paper. It reviews the stages of e-government through which MAs undertaking digitization transition. It seeks to identify potential early adopters via ‘e-maritime maturity” measures. Important blocking factors of non-harmonized basic data and weak business process standardization are considered with illustrations.

A classic change management challenge albeit on a global scale, the ongoing e-government transition in MAs reflects technology and societal trends. E-government change processes have been formalized in academic literature, with two leading models, the Public-Sector Process Rebuilding (PPR) model dating from 2006 and the Layne and Lee model dating from 2001. (T.Almarabeh, 2010, pp. 30-31) Any MA transitioning from paper to e-certificates will go through these steps explicitly or implicitly.

The PPR model identifies four phases of e-government as follows:

i) **Cultivation**: horizontal and vertical integration with government, front-end system, adoption and use of intranet;

ii) **Extension**: extensive use of intranet, personalized web-interface for customer processes;

iii) **Maturity**: abandoning of intranet, accountability and transparent processes, personalized web-interface for customer processes;

iv) **Revolution**: data mobility across organizations, application mobility across vendors, ownership of data transferred to customers

The positioning of most IMO Member State MAs is typically in the first phase ‘Cultivation’. PPR has a government to citizen (G2C) bias and as such is less relevant to MAs, which are serving business stakeholders, so more attention will be paid to Layne & Lee.
Layne & Lee also identify a four stage ‘growth process’. (Heeks, 2015) IMO Member State MAs are typically still in the first ‘catalogue’ and ‘transaction’ phases. Order intake (requests for certificates and/or surveys) are online to a limited extent, while in the vast majority of countries certificate issuance remains paper-based. If digitization has occurred it is typically limited to the paper format certificate issued as a PDF, not an electronic record of data elements in a defined data model. This is the case whether or not the MA is outsourcing to ROs.

**Figure 4: Layne and Lee E-Governance Model**

Source: Heeks

During a 2017 market research study carried out among Paris MOU members with delegated functions to ROs, the author found virtually none had direct computer integration with their ROs, and typically received ‘e-certificates’ in PDF as email
attachments. In Layne & Lee, this could be categorized as vertical integration, albeit loosely defined as the ‘links’ are not proper application program interfaces established through system integration between the information technology platforms of the respective parties. Horizontal integration including ‘Real one-stop shopping’ for shipowners is only available from a handful of MAs, although IMO FAL5-Cir.39, Rev.2 challenges all Member States to reach that stage by April 2019.

The EU ISA2 offers an organizational view with key business processes. Stakeholders are principally concerned with ‘Business Capability’ for exchange and access to e-documents, especially ‘system-to-system back-office solutions’, in other words direct transmission of e-forms from stakeholders to MAs and ‘no touch’ computerized data exchange between government departments – the once only principle put into practice. (JoinUp, 2016) Very few MAs operate like this today, rather most rely instead on physical or electronic document submission, not data submission; this is the breakthrough anticipated from PA3 and the EC eMSW. According to this ‘best practice’ architecture, the ‘state of the art’ MA must offer user-oriented solutions (e-tools like software and websites) to shipowners/operators, masters, PSCOs to manage their interaction with the MA online. MAs must implement solutions for e-certificate storage and managing access rights granted to users.

**Figure 5: E-Documents Reference Architecture : Organization View**

Source: European Commission ISA2
Examples of e-government initiatives, going back at least 20 years are so widespread, that MAs still operating with paper procedures, could justifiably be seen as deliberately blocking global shipping from the transparency, timeliness and traceability that e-government is universally recognized to enable. Furthermore, inadequate e-tools may allow shadowy industry players to avoid regulatory oversight. To dispel such notions, MAs need to get going. Many regional and global e-government initiatives can serve as models for ship e-certificate implementations, such as the United Nations Public Administration Network (UNAP), Department of Economic and Social Affairs (UNDESA) and Division for Public Economics (UNDPE) cooperation on e-governance indexes. These platforms and others at the EU level, include comprehensive interoperable services, frameworks and tools. (JoinUp, 2016) The very impressive UN E-Government Survey 2018 ‘Gearing e-Government to support transformation towards sustainable and resilient societies’ should become obligatory reading for IMO FAL COMM. (UNAP, 2018)

E-government is a dynamic way of delivering public sector services, which is now extensively measured, for example based on the On-line Services Index (OSI) from within the United Nations E-Government Development Index (UNEDI), and internet penetration in the country. (Raconteur.net, 2017, pp. 8-9) Although UNEDI is a well-established and frequently cited UN indicator, it is nowhere visible within the IMO digitization agenda. While this may in part be explained by a G2C bias in UNEDI and a G2B bias in the IMO, the indicators of enabling technologies are relevant to both client constituencies and both organizations. As an illustration of the IMO digital gap, the Country Maritime Profiles (CMP)6 updated in June 2018, included parameters such as gross domestic product (GDP), shipping connectivity index, and happiness index, however made no mention of the UNEDI nor any other e-government measure, nor internet connectivity, nor smartphone/mobile phone penetration, the latter two factors

---

6 CMP serves as the basis for technical assistance needs from IMO Member States, and an upgrade of the tool is under development for delivery in 2019.
being essential tools to support the shift of IMO instrument implementation, governance and enforcement into the digital age. (IMO, 2018, p. 9)

In an attempt to assess maritime ‘e-maturity’ for leading shipping nations, the author has consolidated various relevant indicators. Data has been gathered for IMO Member States including the top twenty ‘e-government’ countries\(^7\) plus the fifteen leading large commercial ship-owner/ship-registry countries; overlap reduces the total to twenty-eight countries. Only four of the ten largest ship-owning countries (Japan, Singapore, South Korea and US) and three of the seven largest ship registries (Liberia (US-based), Marshall Islands (US-based) and Singapore) were among the top-ranking UNEDI score countries. Denmark, Norway and Singapore, all leading e-government, shipowning and flag States countries are strongly committed to e-certificate implementation as testified by their 2017 MOU. (Maritime and Port Authority of Singapore, 2017) Republic of Korea and Norway actively share best practices at the IMO. (Republic of Korea, 2018) (Norway, 2018) It would seem reasonable to expect all top e-government country MAs to be among e-certificate ‘early adopters’, however this is not the case. Beyond the tripartite announcement mentioned, coordination is limited and there is no concerted plan to meet the 2019 deadline.

Table 3 attempts to show which IMO Member MAs live up to their UNEDI score with a compendium of e-maritime indicators, in a first attempt at an ‘e-maritime maturity index’. ‘E-Maritime maturity’ can be inferred by (i) the time-lag (if any) between e-government announcements, and ship e-certificate announcements, (or the lack thereof); (ii) GISIS publishing activity (or lack thereof, which is the majority)\(^8\); and (iii) engagement in FAL COMM working groups. Correlation of the data shows that MAs significantly lag far behind their national e-government policy agenda with few

\(^7\) Israel and Slovenia are excluded, being too small in shipping.

\(^8\) It is recalled that during the 30th IMO FAL COMM meeting in September 2014, members agreed that the GISIS “Survey and Certification” module was to be adapted to add references to Administrations issuing e-certificates, including the list of e-certificates issued by each Administration and any additional information, as considered necessary by the Administration, and to make that information accessible to the general public.
exceptions. OSI maturity overall is not matched by e-certificate issuance. E-certificate announcements are patchy. For Paris MOU and Tokyo MOU countries, the table takes as an announcement proxy, the date of the Third Joint Ministerial Conference declaration inferring e-certificate commitments.\(^9\) Unfortunately, the language is rather vague and notably, the host nation Canada has not yet committed to issuing e-certificates. (Transport Canada, 2017) A key recommendation of this paper, and area for further research is to elaborate such an e-maritime maturity index for all IMO Member States as a tool for themselves and their stakeholders, particularly the ROs. Such an index would be an invaluable tool to identify barriers and enablers for progress. For each country the following data is provided:

i) 2 Letter Country code (International Standards Organization, 2018)
ii) Number of Ships flagged DWT unless * no. of vessels from MA (United Nations Conference on Trade and Development, 2018)
iii) Number of Ships owned DWT unless * no. of vessels from MA (United Nations Conference on Trade and Development, 2018)
iv) On-lines Service Index (OSI) ranking / * UNEDI as per Raconteur
v) On-line Service Index (OSI) score
vi) Internet Users Penetration 2016 as per Raconteur
vii) Digital Trust Environment (Bhaskar Chakravorti, 2018)
viii) National e-Government policy platform announcement
ix) MA accepts e-certificate announcement/ 3rd Joint Ministerial participation
x) MA issues e-certificate announcement (See Appendix 6)
xii) GISIS MA specimen certificate available 20180917 : Red = NA / Green = Available with number of certificates
xii) GISIS MA certificate verification link available 20180917 : Red = NA / Green = available
xiv) IMO FAL COMM e-certificate Working Group meetings attended

\(^9\) ‘Safeguarding Responsible and Sustainable Shipping Joint Efforts for Enhanced Safety, Environmental Protection, and Working and Living Conditions for Seafarers Inter-regional Action to Eliminate Sub-standard Shipping and Promoting a Level Playing Field” May 3-4, 2017, Vancouver, Canada
<table>
<thead>
<tr>
<th>i</th>
<th>ii</th>
<th>iii</th>
<th>iv</th>
<th>v</th>
<th>vi</th>
<th>e-Govt</th>
<th>Digital Trust</th>
<th>e-Certs accepted</th>
<th>e-Certs issued</th>
<th>GISIS Cert.</th>
<th>GISIS verify</th>
<th># of ROs</th>
<th>FAL WG</th>
</tr>
</thead>
<tbody>
<tr>
<td>DK</td>
<td>18,139</td>
<td>39212</td>
<td>1</td>
<td>96</td>
<td>NA</td>
<td></td>
<td>NA</td>
<td>20170504*</td>
<td>20160624</td>
<td>29</td>
<td>29</td>
<td>39 41 42</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>16,658</td>
<td>46384</td>
<td>1</td>
<td>1</td>
<td>93</td>
<td>1996</td>
<td>2.97</td>
<td>20170504*</td>
<td>20180207</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>AU</td>
<td>na</td>
<td>4190</td>
<td>2</td>
<td>0.978</td>
<td>85</td>
<td>1995</td>
<td>2.73</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>39 41 42</td>
</tr>
<tr>
<td>SG</td>
<td>127,644</td>
<td>103,583</td>
<td>3</td>
<td>0.971</td>
<td>83</td>
<td>3.13</td>
<td>20161130</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>CA</td>
<td>na</td>
<td>9082</td>
<td>4</td>
<td>0.956</td>
<td>89</td>
<td>2.17</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>KR</td>
<td>13,974</td>
<td>77277</td>
<td>5</td>
<td>0.942</td>
<td>86</td>
<td>3.29</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>FI</td>
<td>na</td>
<td>2022</td>
<td>6</td>
<td>0.942</td>
<td>93</td>
<td>2000</td>
<td>3.47</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>NZ</td>
<td>na</td>
<td>290</td>
<td>7</td>
<td>0.942</td>
<td>89</td>
<td>2.96</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>FR</td>
<td>na</td>
<td>51464</td>
<td>8</td>
<td>0.942</td>
<td>86</td>
<td>1998</td>
<td>2.83</td>
<td>20170504*</td>
<td>20180208</td>
<td>62</td>
<td></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>NL</td>
<td>na</td>
<td>18116</td>
<td>9</td>
<td>0.927</td>
<td>94</td>
<td>2001</td>
<td>3.64</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>US</td>
<td>53984</td>
<td>10</td>
<td>0.927</td>
<td>89</td>
<td>1993</td>
<td>2.95</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>ES</td>
<td>420*</td>
<td>2455</td>
<td>12</td>
<td>0.913</td>
<td>82</td>
<td>2.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>EE</td>
<td>na</td>
<td>348</td>
<td>13</td>
<td>0.891</td>
<td>91</td>
<td>3.66</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>AE</td>
<td>15045</td>
<td>14</td>
<td>0.891</td>
<td>92</td>
<td></td>
<td>58</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>107119</td>
<td>15*</td>
<td>0.840</td>
<td>88</td>
<td></td>
<td>3.30</td>
<td>20170504*</td>
<td>20170213</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td>39 41 42</td>
</tr>
<tr>
<td>SE</td>
<td>Na</td>
<td>6259</td>
<td>15</td>
<td>0.876</td>
<td>93</td>
<td>3.45</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>JP</td>
<td>34,648</td>
<td>223615</td>
<td>16</td>
<td>0.876</td>
<td>91</td>
<td>3.15</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IT</td>
<td>14,929</td>
<td>19750</td>
<td>17</td>
<td>0.869</td>
<td>66</td>
<td>3.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>NO</td>
<td>18,054</td>
<td>59380</td>
<td>18*</td>
<td>0.804</td>
<td>98</td>
<td>2001</td>
<td>3.43</td>
<td>20170504*</td>
<td>20170516</td>
<td></td>
<td></td>
<td></td>
<td>18</td>
</tr>
<tr>
<td>MX</td>
<td>na</td>
<td>1442</td>
<td>20</td>
<td>0.847</td>
<td>45</td>
<td>2.26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>MT</td>
<td>108,729</td>
<td>2923</td>
<td>30*</td>
<td>0.797</td>
<td>80</td>
<td>NA</td>
<td>20171205</td>
<td>20171026</td>
<td>273</td>
<td></td>
<td></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>RU</td>
<td>Na</td>
<td>22219</td>
<td>35*</td>
<td>0.731</td>
<td>71</td>
<td>2.73</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GR</td>
<td>72,196</td>
<td>330176</td>
<td>43*</td>
<td>0.579</td>
<td>65</td>
<td>NA</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18</td>
</tr>
<tr>
<td>CN</td>
<td>265,280*</td>
<td>183094</td>
<td>63*</td>
<td>0.768</td>
<td>52</td>
<td>1.73</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>PA</td>
<td>335,313</td>
<td>1471</td>
<td>99*</td>
<td>0.333</td>
<td>45</td>
<td>NA</td>
<td>20170801</td>
<td>20170801</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>ID</td>
<td>18,273</td>
<td>24852</td>
<td>116*</td>
<td>0.362</td>
<td>20</td>
<td>2.83</td>
<td>20170504*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>MH</td>
<td>237,807</td>
<td>1442</td>
<td>156*</td>
<td>0.029</td>
<td>20</td>
<td>NA</td>
<td>20170801</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>LR</td>
<td>223,655</td>
<td>215</td>
<td>170*</td>
<td>0.239</td>
<td>9</td>
<td>NA</td>
<td>2006</td>
<td>20161012</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>42</td>
</tr>
</tbody>
</table>

* UN-EGDI ranking / Compiled by B.Cosgrave based on cited sources
User engagement and adoption are paramount for successful implementation of e-certificates. So far this has been a big flop for e-certificates as illustrated by very low penetration. Operational efficiencies from G2B e-procedures should be of great interest to shipowners and their agents, given their challenging financial situation. However benefits need to be financially measurable and better communicated. The EU has enumerated benefits from Maritime Single Windows being 22-25 million staff hours in 2020-2030 or EUR 625 to 720 million in the EU 28 Member States from reduction in administrative burden for shipping operators. In addition environmental benefits include modal shift from road to waterborne traffic of 3,395 million ton-kilometers in 2030 resulting in an overall reduction of 1.88 MT of CO2 emissions relative to baseline. All told, around EUR 145 million of indirect benefits over 2020-2030. (EC, 2018, p. Legislative Financial Statement p.3) PA3 has enumerated potential timesaving per each PSC inspection of 1.5 to 3 hours from online certificates checked in advance. Such Master/crew time-saving will allow greater concentration on safe navigation. Lower detention rates due to invalid certificates which can be corrected in advance, should also lead to cost avoidance, however this is as yet unquantified.

Based on other industry examples, multi-country change management programs are greatly facilitated by personal relationships among stakeholder C-level leaders, the fewer the better. When leaders are aligned, major industry shifts can be achieved during short timeframes, typically two years. E-certificate ‘thought leaders’ might be found in the commercial ships category of 50,155 vessels (see Appendix 7). This category is largely controlled by the ten largest ship-owning communities, and the seven largest flags. A target group of fifteen stakeholder representatives could make a head-start with e-certificate deployment on about 60% of the world fleet. A public-private partnership between these flag States and shipowner communities, could help accelerate adoption, and realize benefits rapidly especially given that a few countries (DK, KR, NO, SG) are already onboard.
5. The IMO Approach to Electronic Certificates

In the IMO, Interim guidelines on e-certificates were issued initially 18 Apr 2013, revised to become Guidelines on 7 Oct 2014, and revised again 20 Apr 2016 when FAL 40 adopted the Guidelines for the use of electronic certificates (FAL.5/Circ.39/Rev.2). Acceptability and interoperability are core concerns of users, hence the Committee also approved the draft amendments to resolution A.1052(27) on Procedures for port State control (FAL 40/6, Annex 2), clarifying the validity of e-certificates during a port State control inspection. A Correspondence Group, the IMO FAL COMM Working Group on Electronic Means for the Clearance of Ships (WG9) is tasked to drive adoption with some 30 members and observers. This group is still deliberating, several years after forming, and has not yet adopted a program management approach to systematically identify and dismantle barriers. There is no evidence that FAL COMM have considered e-certificate reference architectures such as that of ISA2, nor are there key performance indicators to monitor deployment progress. Concerns that technology is under-exploited in the IMO working procedures is a constant refrain, repeated in a recent paper from a dozen Member States (Antigua and Barbuda, 2018) These concerns seem justified, in light of WG9 progress thus far. Notably, in the recently elaborated FAL COMM terms of reference there are no explicit references to digitization, modernization of administration nor e-government among its seven objectives. In thirty-two pages of instructions, the internet is mentioned only once, under “…5.11 Correspondence groups should utilize modern communications technology, such as the Internet, as much as possible….“ (IMO, 2018, p. 11)

TOOP PA3 offers a framework against which the IMO efforts can be benchmarked. TOOP includes pilot projects, a generic federated Once Only Principle architecture, and investigates drivers and barriers. Clearly this program management approach is missing in FAL COMM. IMO focuses on the document itself, defining key terms. However there is no commitment to a e-certificate data model standard and a deadline
for data element standardization (2021) was only adopted reactively after alarms were raised (see below).

According to the ISA2 model (Figure 6) a global e-certificate standard should be comprehensive including: an identifier scheme, an e-document meta-model, an e-file meta-model, container meta-model, archiving meta-data, descriptive meta-data, routing meta-data and transactional data. (JoinUp, 2016) WG9 discussions have touched on topics such as e-certificate content, meta-data and e-signatures. Document management systems for multiple certificates for a single ship are left to the MAs and their ROs, which hampers standardization.

Figure 6: E-Documents Reference Architecture: Semantic View

Source: European Commission ISA2

Where standards have been elaborated, fragmentation and lack of interoperability are common, or else standards are simply ignored. For example, the ISO 28005 Security Management Systems for the Supply Chain – Electronic Port Clearance (EPC) is a ‘Maritime Single Window’ standard. It is comprised of two parts: ISO 28005-1:2013 message structures and ISO 28005-2: 2011 core data elements. It is developed by the technical committee: ISO TC 8/SC11/Intermodal and Short Sea Shipping, with the secretariat provided by the Korean Agency for Technology and Standards. Published in March 2013, and revised in 2018, it is not clear where and when this standard has been adopted by IMO Member States, except Republic of Korea (see above). Encouragingly, it has been used for an eMSW pilot within the European Maritime Safety Agency (EMSA). The most blatant renunciation of standards found by this author dates from 2011 and the FAL.5./Circ.36, in which it is clearly stated:
“2.3 No standards defined: These guidelines do not define any particular standard for implementing a single window. They point to different internationally recognized standards that are available and that can be utilized as appropriate.” (IMO, 2011)

This standards avoidance is inconsistent with the historical feedback from industry stakeholders, such as the findings from an EC public consultation which elicited over 95% support for e-maritime standards to be prioritized in policy implementation. (EC DG MOVE, 2010)

**Figure 7: E-Maritime Policy Implementation Stakeholder Feedback**

![E-Maritime Policy Implementation Stakeholder Feedback](image)

Source: EC DG MOVE

A laudable effort to tackle disparate standards across various shipping functional siloes comes from the International Taskforce on Port Call Optimization (ITPCO) out of the International Harbour Masters Association (IMHA). Their project to harmonize port entry data consolidates standards from the International Hydrographic Organization (IHO), International Standards Organization (ISO), World Meteorological
Organization (WMO), the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) Baltic and International Maritime Council (BIMCO) and GS1. ITPCO / IMHA deliverables cover functional data definitions for static berth conditions and dynamic state events in the berthing process. These data standard definitions were developed after strong pressure exerted on port authorities by the oil majors and carrier lines. Useful deliverables were announced in 2018 based on work ongoing since 2006. The IMHA proudly states that definitions will be incorporated in the next version of the Mariners Handbook (NP100). (IHMA, 2018)

The fact that multiple data systems, for example GISIS, EQUASIS and THETIS (among others) operate alongside each other, would be less problematic if at least the meta-data definitions could be harmonized, otherwise too much energy is expended to submit the same data in different formats to various platforms, as is currently the practice. Recalling the definition of an e-certificate as a data file comprised of data elements certified by the relevant authority, operational issues related to data harmonization are critical. While standards have emerged for various parts of the extremely broad and complex business processes entailed in shipping, these are unable to work inter-operably, if from the outset they are conceived, designed and implemented based on heterogeneous data element definitions. The multiplicity of datasets and unharmonized data elements in use has been recently flagged to the IMO with a call to elaborate a Common Maritime Data Structure (CMDS) consolidating the plethora of industry data element definitions (see Figure 8). (BIMCO, 2017)
**Figure 8: Examples of Heterogeneous Data Standards in Shipping**

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Description</th>
<th>ISO 28005</th>
<th>UN EDIFact</th>
<th>WCO ID</th>
<th>IACS R75</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship Name</td>
<td>Given name in the ship registry</td>
<td>ShipID.ShipName</td>
<td>C222:8212</td>
<td>T005</td>
<td>SHIP_Name</td>
</tr>
<tr>
<td>Call Sign</td>
<td>Call sign of the ship: sequence of letters and numbers, unique to each ship, by which ship can be identified, usually in radiocommunications</td>
<td>ShipID.CallSign</td>
<td>C076:3148</td>
<td>Type (253)</td>
<td>SHIP_Call_Sign</td>
</tr>
<tr>
<td>IMO Number</td>
<td>Unique ship identification number assigned by Lloyd’s Register/Fairplay in accordance with IMO Res.A.600(15)</td>
<td>ShipID.IMONumber</td>
<td>C222:8213</td>
<td>T006</td>
<td>SHIP_IMO_Number</td>
</tr>
<tr>
<td>MMSI Number</td>
<td>Identifier used by maritime digital selected calling (DSC), automatic identification systems (AIS) and certain other equipment to uniquely identify a ship or a coast radio station</td>
<td>ShipID.MMSINumber</td>
<td></td>
<td>Type (253)</td>
<td></td>
</tr>
<tr>
<td>Comments</td>
<td>Any other information related to ship identity</td>
<td>ShipID.Comment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: BIMCO

MAs typically outsource part or all of their certificate activity to one or more ROs (see Table 3). Although an in-depth review of RO business practices is highly relevant to this study, length restrictions of this paper preclude it. Alternatively a consideration of CLASS standardization activity is provided. The International Association of
Classification Societies (IACS)\textsuperscript{10}, regarded as best practice operators, has expert groups for data models, e-certificates and cyber-security. IACS elaborated the Unified Data Exchange Format (UDEF) with a twenty page specification document in June 2001, commonly referred to as ‘Recommendation 75’ (Rec. 75). The standard was completely revised in Feb. 2015, corrected in Feb. 2016 and Revision 2 was issued Dec. 2016. Rec.75 refers to thirty-eight certificate types, fewer than the RU report and GISIS. Although presented to IMO as document MSC 95.21.6, it has not been adopted as a standard by FAL COMM for their e-certificate guidelines, and it is not universally adopted by MAs that outsource to IACS members. (IACS , 2017).

\textsuperscript{10} American Bureau of Shipping (ABS), Bureau Veritas (BV), China Classification Society (CCS), Croatian Register of Shipping (CRS), Det Norske Veritas Germanischer Lloyd (DNV GL), Indian Register of Shipping (IRS), Korean Register of Shipping (KR), Lloyd's Register of Shipping (LR)
6. Digital Initiatives in Adjacent Sectors

Multi-country, multi-lingual, public/private initiatives in other domains suggest that IMO Member States can do far better in advancing along the digital agenda, with significant advantages to be gained. Examples from container shipping, and customs clearance, illustrate that ship e-certificate deployment is anywhere from five to fifteen years behind these adjacent business processes.

In 2001 with the advent of e-commerce, six leading carrier lines\(^\text{11}\) joined forces to build a common platform for the electronic exchange of booking and shipping instruction data between shippers and carriers, branded ‘INTTRA’. Since then, the platform has grown dramatically to now serve some 30,000 shippers on 60 carrier lines and Non-Vessel Owning Common Carriers (NVOCCs) in 200 countries. (Recalling that 50,000 commercial vessels are owned/flagged in 15 countries, e-certificate deployment faces a fraction of the complexity.) Varying connectivity solutions among users is accommodated by INTTRA with a range of options for data submission and review including online via the World Wide Web; secure website via an application program interface and the EDIFact standard. There is also a document conversion process; a software application that can be installed on the shipper/forwarder’s laptop or desktop computer, via which data entered into the home system is transmitted to INTTRA as an e-mail attachment. (INTTRA, 2018)

In the customs domain, the EU Directorate General for Taxation and Customs Union (DG TAXUD) project to implement a Unified Customs Code in all EU Member States which is underway since 2013 has chosen to follow the WCO lead focusing on data elements, harmonizing them, and using data models appropriate to the reporting requirement. This allows to clearly identify those data elements needed for each verification use-case. Data elements can be re-used and shared between interested parties, in a more flexible manner than documents.

\(^{11}\) CMA-CGM, Hapag-Lloyd, Hamburg Sud, Maersk, Mediterranean Shipping Company, United Arab Shipping Company
Referring back to the RU analysis of IMO certification obligations, although the report identified various challenges it missed the point that ‘data’ could be part of the solution. There is no mention of ‘data’ nor ‘data element’ in their report, rather it is proposed that a new ‘dedicated legislative tool’ might be helpful, however adopting such an instrument through the IMO process would be extremely protracted at best and interminable at worst.

Successful implementation of the FAL.5/39 guidelines can release PSCOs and crews from the drudgery of paper certificate review. How the released PSCO time and energy will be re-directed to new duties, (e.g environmental compliance) and whether this will result in higher standards of shipping safety and pollution control is the promise to be realized from the digitization process. Since the guidelines were issued, IMO Member States and stakeholders have been grappling with their ramifications. With the experience of first movers, the IMO has sufficient evidence that e-certificates deliver tangible benefits to issuers and users. Attendance to FAL COMM working groups is not an indicator of genuine e-certificate engagement or deployment. The IMO should take more initiative to measure the e-maritime maturity of its member states, with an appropriately constructed index that can provide stakeholders a tool to track delivery against government commitments rather than hoping for eventual fulfilment of ratification obligations.
7. **Fraud & Trust Aspects of Electronic Certificates**

This section of the paper considers the issues of fraud and trust. It starts with data on the frequency of certificate and documentation deficiencies to provide some scale to the issue. The matter of fraudulent registration will be discussed based on very current developments. Cybersecurity will be touched on for the sake of completeness, but not over-emphasized as the subject is vast and goes beyond the scope of this paper. This will be followed with a summary of factors to enhance trust. Finally an analysis of e-certificates as components of the “Future Internet”, the more robust and reliable technology infrastructure than can support ubiquitous electronic operating procedures will be offered as a vision going forward.

**Figure 9: Deficiencies in Port State Control Inspections 2016**

![Pie chart showing deficiencies in Port State Control Inspections 2016](source: IMO Secretariat)
The consistency with which ship certificates and documents irregularities (for reasons legitimate or otherwise), arise in ship inspections justifies seeking to improve the status quo with the latest technology. In the most recent PSC inspection data from 2016, ship detentions for all causes represented 3.19% or 2,814 vessels out of 88,291 initial inspections among the ten PSC regimes, down from 3.27% in 2015. While 64.1% of all deficiencies relate to SOLAS (excluding deficiencies related to certificates and documents), the next most important factor at 9.8% is ship's certificates and documents (all instruments) followed by 5.8% due to MARPOL (excluding deficiencies related to certificates and documents). Figure 9 illustrates the distribution of deficiencies globally for 2016. (IMO Secretariat, 2018, p. 7)

While the instance of certificate deficiencies vary across MOUs, they are a persistent challenge. For example, this category represent more than 6,000 deficiencies annually recorded by the Paris MOU over the past five years and in 2016 instances increased by 7.7% to 6,779 from 6,295 in 2015. (Paris MOU, 2017, p. 18) The Black Sea MOU confirmed that in 2017, out of 5,112 inspections, some 3,018 inspected vessels with 21,006 deficiencies, included 1,292 or 6.15% for documents and 421 or 2% for crew certificates. (Black Sea MOU, 2018, p. Annex p.2)

The extreme case of non-compliance is fraudulent ship registration. The UK Fraud Act 2006 Section 1(2) defines three categories of fraud: Section 2 (fraud by false representation); Sec.3 (fraud by failing to disclose information); Sec. 4 (fraud by abuse of position). Fraudulent ship registration and fraudulent documents relate to all three definitions given s.2 covers false representation of ship documents and certificates to public authorities such as PSCO and private actors such as insurers (if indeed the vessel is insured); s.3 pertains to the legal duty of shipowner and captain to disclose information about the vessel, which will have been falsified, and again s.4 covers shipowner and captain as persons in a position expected to safeguard or not to act

---

against the financial interests of another person – in this case, all parties in the shipping value chain such as suppliers, crew. (Todd, 2010, pp. 2, Ch2) The practice of fraudulent ship registration, which has been linked to piracy, is persistent and troubles several countries. In 2017 alone, the Democratic Republic of Congo cited 73 vessels fraudulently flying its flag, Fiji had 91 such cases and the Federated States of Micronesia (not an IMO Member State) had 150 fraudulent ships. IMO measures to combat maritime fraud and illegitimate registrations include: IMO Ship Identification Number Scheme (Resolution A.1117(30); IMO Unique Company and Registered Owner Identification Number Schemes (Resolution MSC 160(78)); Continuous Synopsis Record; measures to prevent ‘Phantom’ ship registration (Resolution A.923(22) and a recommended ‘transparency’ procedure for transfer between flag States (MSC/Circ. 1140/MEPC/Circ. 424). But these measures are deemed insufficient, particularly when fraudsters avail themselves of new tools such as fake websites. The urgency of the matter is summarized by IMO member states 13 as follows: “…existing mandatory and non-mandatory instruments of IMO or the UN are not adequate to help prevent fraudulent registration of ships…” . They are calling for an urgent work item to address this modern-day piracy issue, albeit without explicitly enumerating digital technologies as root cause nor possible solution. (IMO Member States: CY, DRC, FI, DE, MO, SP, VA, 2018, pp. 1-6)

Fraud and corruption of the ship documentation process can at times find its source within the MA. Considerable academic research has focused on the utility of ICT tools to frustrate state corruption, providing further justification for broader e-government adoption in the maritime sector. The team of Shim & Eom are leading here with robust studies grounded in considerable data analysis. In their research they cite studies confirming e-government programs as successful anti-corruption tools in Argentina, Chile, India, South Korea and Russia, notably all important maritime countries.

13 Cyprus, Democratic Republic of Congo, Fiji, Germany, Morocco, Spain, Vanuatu
methodology includes country corruption measures from Transparency International, something to be considered in the IMO CMP. (Eom, 2009, p. 105)

The spectacular growth of internet users from 400 million in 2000 to the current level of 4,021 Billion or 53% of global population penetration (Kemp, 2018) has been met with a similar explosion in service offerings and service providers. The coincident growth of data management breaches has fractured user trust and elicited belated regulatory responses of varying severity. This new operating paradigm is referred to as the Future Internet (FI). The FI environment is characterized by ‘…a new generation of service (e.g. a hybrid aggregation of content and functionality), service factories (e.g. personal and enterprise mash-ups), and service warehouses (e.g. platform as a service). One specific service instance may thus be created by multiple service development organizations, it may be hosted and deployed by multiple providers, and may be operated and used by a virtual consortium of business stakeholders.’” Evidence that greater sophistication is needed comes from the escalation of ‘cyber-threats’ from hacking in public and private sector. To ensure the trustworthiness of new services Joosen et al. propose they be built under the confluence of software engineering, service engineering and security engineering disciplines. (Wouter Joosen, 2011, pp. 177-178)

The FI challenges public and private sector alike. MAAs must move beyond the initial phase of e-government to deploy already widely available tools for data mining and ‘big data’ and toward ‘i-government’ which will be rooted in the ‘Internet of Everything’ (Kamolov, 2017). An sample regulatory response is the EU Directive on Security of Network and Information Systems (‘NIS’ Directive) which entered into force August 2016, obliging all EU Member States to elaborate national ‘cyber’ strategies, with coverage of essential services including key industry sectors. (ENISA, 2016) This is a policy shift from the prior focus on public sector ICT infrastructure. For example the Republic of Cyprus national cyber strategy in 2012 makes no mention of maritime, while the Danish Center for Cyber Security strategy from 2018 forward has focused on six key industries including maritime. (OCECPR, 2012) (Fiedel, 2018).
Most of the software tools widely used in society pre-date the FI, and this is particularly true in shipping. Widening digital technology adoption and co-incident change to standard operating procedures are over-whelming the maritime private sector which is particularly under-invested in digital systems, leaving them highly vulnerable to cyber-fraud as their systems are weak, easily hacked and response mechanisms almost non-existent. (Sorensen, 2018). Size is no defense, as the attacks on Maersk in 2017 illustrated, leading to a root and branch overhaul of their information technology. (AP Moller Maersk, 2018). Shipping has now recognized the dangers. Based on a proposal from the US (United States, 2017), the IMO (2017) Resolution MSC.428(98) *Maritime Cyber Risk Management in Safety Management Systems* was adopted to incorporate cyber-risks within the ISM Code and make compliance obligatory as from 2021 (and one year thereafter for audit and PSC). (IMO, 2017) A copy of the resolution is provided in Appendix 8.

However, strong resistance to change generates persistent trust challenges among MA internal and external stakeholders. Okut-Uman identified three basic imperatives to generate confidence in electronic media: i) Valid laws of evidence providing for the admissibility of electronic documents and electronic signatures in legal proceedings; ii) Electronic (digital) signatures having legal effect and validity and iii) A trusted business environment based on public key infrastructure (PKI). (Okut-Uman, 2002, p. 11) The first two have been dealt with in part three of this paper. PKI is a generic all-encompassing term referring to a suite of e-tools and methods that replace handwritten signatures. It is complex topic, that requires an extensive technological explanation to do it justice. The author found the most clear and definitive report on the subject to be an UNCITRAL that covers technology and legal concepts (and runs to 114 pages). By way of introduction, it cites: “ “Digital signature” is a name for technological applications using asymmetric cryptography, also referred to as public key encryption systems, to ensure the authenticity of electronic messages and guarantee the integrity of the contents of these messages. The digital signature has many different appearances, such as fail stop digital signatures, blind signatures and undeniable digital signatures. (UNCITRAL, 2009) Another treatment, albeit even more technical is
provided by Brands. (Brands, 2000) Referring again to the ISA2 model, PKI ‘building blocks’ are illustrated in Figure 9.

**Figure 9: E-Documents Reference Architecture: Technical View Infrastructure**

Source: European Commission ISA2

PKI tools and methodologies are typically defined for e-government at a national level and can be adopted by the MA. It remains to be seen whether various national tools offer global inter-operability or whether a common standard needs to be adopted by issuers. Mutual recognition between MAs and ROs as certificate authorities is underway. It is debatable whether IMO guidelines qualify as an adequate accreditation mechanism. Broader global implementation will prove this point.

Other factors influencing trust include the robustness, security and affordability of connectivity available to MAs particularly PSCOs. Given e-certificates are targeted at the G2B segment, affordability is not really an issue, but the argument is used frequently by detractors. While unique mobile phone users now number 5,135 Billion or 68% of global population penetration, service access is no longer the issue but quality varies according to geography, driven by the competitiveness of service providers. 2016 data for consumer connectivity in some sixty low and middle-income countries confirms that affordability remains a challenge in two-thirds while one third of the group has made measurable progress. (A4AI, 2017).
A useful tool to support all maritime stakeholders in this domain would be Global Maritime Connectivity Index (GMCI), as a complement to the e-maritime maturity measures in Table 3. The GMCI would measure basic performance indicators for digital connectivity in major global ports and the 200 nautical mile limit associated thereto. In an initial phase the geographic scope should include the 100 EU ports defined was ‘Core Ports” by DG MOVE. This will be of keen interest to EMSA. Subsequently it could be expanded to the top 100 ports globally and eventually main ports in the ASEAN countries and at least one major port per IMO member state. The drivers for reliable, accessible information about digital connectivity in maritime locations are myriad including maritime single windows, autonomous vessels, digitized customs clearance processes, remote operational control and maintenance of maritime equipment, and finally sea traffic management and port collaborative decision-making. The GMDI would be of interest to ship operators, nautical equipment vendors, policy makers and regulators. It should include multi-technology coverage such as fixed wireless, mobile communications, satellite communications and low-power wide-area networks. Measurement of operational parameters such as signal strength, interference would be invaluable to ensure that the growing scope of maritime and nautical applications and e-tools can function properly.
8. The Future Internet of Ships

Looking forward, in a broader context, e-certificates are an enabling but insufficient factor for the digitization of shipping as a whole, which can be referred to as the Future Internet of Ships (FiOoS), being the maritime sector component of the FI. The digitization of ship certificates can be presented as a specific application of the generic Future Internet Enterprise System (FInES) as elaborated by Angelucci et al. The FInES is defined as “…a progressive implementation of a rich, complex, articulated digital world that reflects the real business world, where computational elements, referred to as FInER (Future Internet Enterprise Resources) will direct, act and evolve according to what exists in the real world.” (Daniella Angelucci, 2011, p. 407) Hereafter the FiOoS is conceived as an information technology system architecture comprised of multiple variables, e-certificates being one of them, interacting to achieve the digitization. The FiOoS as presented here encompasses internet of shipping services (e.g. sea traffic management voyage management and port collaborative decision making (STM Validation Project, 2018)), internet of shipping things (e.g. smart ships (autonomous vessels being the extreme example), smart objects enabled with radiocommunications to facilitate remote monitored such as engines and pumps), internet of shipping knowledge (documents online in real-time i.e. IMO GISIS modules), internet of shipping people (digital identities for seafarers /fishers). All of these aforementioned categories are subject to some degree of certification, frequently with a certificate attesting to compliance. The FiOoS as a technology paradigm illustrates the shift of management, planning and execution of shipping to new services, new tools, new software packages, new interfaces, and new user interaction solutions.

The FiOoS can be expressed as a function of Future Internet of Ship Resources (FiOoS R) which include concrete tangible things such as a ship, pump or engine, as well as intangible things, such as training course, business process, marketing strategy, and in some cases the tangible migrating to the intangible, such as paper ship certificates.
transitioning to e-certificates which are in effect data files. The FIoSRs can be expressed in the following manner:

FIoSR is a 5-tuple:  
\[ FIoSR \ (i.e. \ e-Certificate) = (FID, GR, M, B, N) \]  
defined as follows:

FID: *FInER (unique) identifiers* of the FIoSR, defined according to precise universally accepted standards (e.g. internet addresses according to the IPV6 standard; URI - Universal Resource Identifier or any ENS – entity name system);

GR: *graphical representation*, (e.g. GIF, 3D Model, JPEG, Video);

M: *memory* which can range from ROM (read-only memory) with basic info to complex knowledge of all components, properties and lifecycle history;

B: *behaviour* is a functional capability of the FIoSR structured in line with profile (IOPE – input, output, processing, effects) and model (workflows), may be self-monitoring;

N: *networking* – specifications of all possible interactions the FIoS can achieve;

(Daniella Angelucci, 2011, p. 413)

Hereafter we considered a ship e-certificate using the FIoSR aspects listed above:

FID: with respect to identifiers, the transition to the use of various unique identifiers is already underway with tracking identification numbers (TINs) used for verification of authenticity and validity either on MA websites or via the GISIS Survey and Certification module. At present the numbering systems used are national and not harmonized globally. The functionality of unique identifiers can be extended when they are linked to Internet enabled names, numbers and addresses. These properties are governed globally by the Internet Corporation for Assigned Names and Numbers (ICANN). For example, the generic top level domain name (gTLD) ‘.ship’ could be

\[ ^{14} \text{While ICANN may not yet have allocated the ‘.ship’ top level domain, at least the ICANN community is very aware of shipping, but perhaps for the wrong reason. On 1} \]
exploited by FIoS related websites and services. Internet addresses can be allocated according to the Internet Protocol Version 6 (IPV6) standard. Functionalities could be extended through closer coordination between the shipping and Internet communities however it appears that very little of this linkage work has been done so far. In the case of the gTLD, attempts have been made since 1999 to gain management rights, but to date the ‘.ship’ and ‘.vessel’ domain names do not yet exist (restricted rights to domain names ‘.boats’ and ‘.yachts’ were allocated in 2016 (Domain Name Wire, 2016)). (Internet Assigned Numbers Authority, 2018)

GR: The information contained in a ship survey report is not limited to prose nor data. Pictures and videos are actively encouraged by PSC MOUs. The Paris MOU even has a contest, ‘Caught in the Net’ for the most telling image of non-compliance (Paris MOU, 2018). Hence e-certificates ideally should have graphical representation properties. In the case of large naval architecture plans this can present storage and behavioural challenges. It may be relevant for shipping experts to liaise with the ISO/IEC technical committees that govern standards for this area.

B: Behaviours of an FIoS e-certificate could include input data (CLASS parameters) being interoperable with output data needs (port berthing details) and software tools that manage workflows to which the vessel is subjected. Self-monitoring of the e-certificate can include alarms to the issuer (MA) and the user (shipowner) in anticipation of expiry.

September 2016, a fire broke out in the containership *CCNI Arauco*, while docked in the port of Hamburg, resulting in two containers filled with technical equipment en route from the ICANN 56 meeting held in Helsinki, Finland to the ICANN 57 meeting scheduled for Hyderabad, India. One of the containers which was undamaged, was off-loaded to another ship and made its way to India. The other container, stuffed with electronic office and computing kit was damaged and detained in Hamburg. Due to maritime law, inspections by German authorities and the shipping company’s insurance adjusters, release of the property could take several months to several years. [https://www.icann.org/news/blog/fire-on-cargo-ship-affects-it-equipment-bound-for-icann57-hyderabad](https://www.icann.org/news/blog/fire-on-cargo-ship-affects-it-equipment-bound-for-icann57-hyderabad)
M: The memory properties of e-certificates will facilitate auditability. Standards can support the interoperability of e-certificates with limits on certificate size if appropriate. Memory capacity via ‘cloud computing’ can provide adequate memory capacity for all parties engaged in global shipping. Cloud based services are making real-time data transfer a normal business practice. Shipowners are increasing interested to assess how they can exploit existing connectivity and messaging formats to ensure rapid adoption of e-certificates for improved interfaces to ports and other parties in the shipping value chain. Shipping stakeholders seek to better understand the product and service options presented by e-certificates. CLASS are particularly interested by maritime ‘cloud’ for internal operations and for service offerings to customers.

N: The myriad networking interactions of a paper ship certificate have been alluded to in this paper. Once fully digital, the e-certificate functions may expand for example to include embedding them as supporting documents in smart contracts using distributed ledger technologies for marine (re)insurance, or ship finance. The FiOS e-certificate will be enabled for interactive state events, with data being stored, shared and computed based on the particular stage of the shipping business process, or the demands of a particular user.

The FiOS would entail the transition of physical processes and equipment shifts, for example a capital good sale (buy a ship, buy equipment on a ship) to a solution sale (buy the services of a ship, buy the services of the equipment on the ship including real-time monitoring and when necessary (remote) maintenance). This transition is ongoing across all transport modes. For the FiOS to function properly all entities defined as FiOSR must be able to act as computational units. Critically these units require the capability of a ‘networked identity’, hence the push for encrypted data on certificates that is comprised of harmonized data elements that can be interoperable in the various software tools in the myriad business processes of the global shipping value chain.
9. Conclusion and Recommendations

In conclusion, this paper has presented the transition of ship certificates from paper to digital formats, which is taking place at a rate and volume that is inferior to the digital ambitions of the IMO and e-government adoption in the public sector as a whole. While poor penetration of e-government in maritime administrations may be explained in part by budget prioritization, it is also a reflection of a digital leadership deficit in shipping and its decision-making bodies. To ensure IMO targets for the ‘electronic clearance of vessels’ are realized, a program management approach with multi-country indicators, platforms and tools, is needed. Sample existing tools, and suggestions for new indicators have been provided.

This paper has illustrated that e-certificates for ships as an e-government program can accelerate administrative procedures, ensure more complete data capture, and better control implementation, while also generating measurable economic benefits for shipowners. Although the technical solutions are deployed by the MA, stakeholder engagement and adoption are essential for success and need adequate attention through effective change management procedures. Select approaches to e-certificates by IMO Member flag States, their ROs, and port States and their PSCO inspection activities have illustrated the status quo as at publication.

The conclusions reached suggest that ‘first mover’ IMO Member States have succeeded. E-certificate adoption could benefit from closer ties between maritime administrations and their national e-government initiatives. Global implementation could be accelerated with large scale multi-country deployments. The following recommendations are offered on the basis of the research and findings of this paper:

1. **E-Certificate Public Private Partnership**: launch an initiative with fewer than 15 members (including CLASS, Shipowner representatives, and MAs) committed to a 24 month time frame to ‘kick-start’ e-certificate deployment in the shipping industry (possibly focus on Commercial Vessels to start), while following relevant parts of the ISA2 architecture and the TOOP methodology. This could mimic the Global Maritime Energy Efficiency Partnerships (GloMeep) [http://www.imo.org/en/MediaCentre/PressBriefings/Pages/17-GIA-GloMeep-launch.aspx](http://www.imo.org/en/MediaCentre/PressBriefings/Pages/17-GIA-GloMeep-launch.aspx)
2. Global e-Maritime Maturity Index: supported by the IMO, academia and/or industry, generate an annual ‘e-maritime maturity index’ for all member states, including enabling technology measures such as smartphone penetration, connectivity access, and corruption measures from Transparency International. (This may have a knock-on implication for the IMO Member State Audit Scheme).

3. Global Maritime Connectivity Index (GMCI), opportunity for a sponsored indicator of digital connectivity in major global ports and the 200 nautical mile limit associated to the location, starting with EU 100 ‘Core Ports” expanded to top 100 ports globally, and eventually at least one major port per IMO member state. Could be a vendor led initiative.

4. IMO Technical Assistance: leverage UNEDI, UNAP and UNDES e-government programs in IMO Member States. Maritime Administrations, making the linkage between successful e-government programs and Maritime Administrations that are not yet digital.

5. World Maritime University: incorporate digital technologies, e-skills and project management in all disciplines in order to heighten the digital competence of the shipping industry. The MLP specialization to have dedicated e-government content so that students link their policy and legal activities to the electronic age.
References


Danish Maritime Authority. (2018, 2 2). Online control of certificates could lead to faster PSC inspections. *Press Release*. Valby, Copenhagen, Denmark: DMA.


https://ict4dblog.wordpress.com/2015/03/23/a-better-e-government-maturity-model/


RINA. (2015, October 9). Certified E-document Authority, a Business Concept. CEDA. Genova, Genova, ITALY: RINA.


Bahamas Approved Nautical Inspectors, Shipowners, Managers and Masters.

Information Bulletin. BMA.


Appendix 1: Physical Inspection of Ship Certificates & Documents

Danish Port State Control officer inspecting ship certificates
(Danish Maritime Authority, 2018)

Ghana PSCO Checking Ships Certificates & Documents
(Abuja Memorandum of Understanding on Port State Control, 2015)
Appendix 2: Sample Certificate of Registry, Kingdom of the Netherlands

IN NAAM VAN ZIJNE MAJESTEIT DE KONING DER NEDERLANDEN
IN THE NAME OF HIS MAJESTY THE KING OF THE NETHERLANDS

Hierbij wordt verklaard dat:
This is to certify that:

het Motorvaartuig
the Motor craft

getuige:
gentooer:

STALSCHIP
STEEL

staal (NEDERLAND)
STEEL (THE NETHERLANDS)

in het jaar:
in the year:

1988

hebbende:
having:

DEK

voorbewogen door:
propelled by:

Engine 1
Engine 2

met een vermogen van (kW):
with a rated capacity of:

850
124

motornummer(s):
motor number(s):

1235657
1234666

de bruto tonnage is:
de netto tonnage is:
gross tonnage:
net tonnage:

250

Appendix 3: Vessel Registration in Liberia

VESSSEL REGISTRATION IN LIBERIA – FLOWCHART

How to register a Vessel in Liberia?

CONTACT ANY OF OUR REGIONAL OFFICES WORLDWIDE and coordinate preparations with Class, LR-Fairplay, P&I, Crew Agent and Banks

IMO

Class Society

LR-Fairplay IMO members

P&I CLUB Insurance

CREW Certification

FINANCING Mortgage

DEPUTY COMMISSIONER OFFICE - DCO

REGISTRATION DEPARTMENT

E-mail: RegistrationDCO@lroc.com

CPF Cover

- Bonus Card

- GLC Blue Card

- WRC Blue Card

Submit applications and qualifications directly or through Registered Cowing Agent

Owner to register a Liberian entity (Corporation, LLC, etc.)

Owner to register an existing foreign company as a qualified Foreign Maritime Entity (PFME) in Liberia

- vessel Name verification

- Review of all applications and other documents as per RLM-190, Chapter VI

- Official Member, Call Signs, MMSI, EMD, MPA, DGC

- Coordination with other departments

We will guide you through the process

Owner to authorize Flag Classification Society to email any flag required Class records and survey reports to The Liberian Registry Technical Digit.

CORPORATE REGISTRY corporate@lroc.com

DEPUTY COMMISSIONER OFFICE - DCO

MORTGAGE DEPARTMENT

Mortgage@lroc.com

MANAGER

TECHNICAL

safety@lroc.com

SECURITY

security@lroc.com

AUDIT

audit@lroc.com

LEIT

leit@lroc.com

INMARSAT

inmarsat@lroc.com

VESSEL CERTIFICATES

VesselCertification@lroc.com

SEA-DOCS

seado@lroc.com

IMO, SOLAS, Clas disc review, Towed ship/grounding, Dispensations

Managing Safety Code, ISM Code, PSC, Distraction Prevention

EPL Ship Security Plans approved, Armed Guards

Flag Safety Various, MLC, ISM, EPS, Harmonized Codes

Flag Safety Various, MLC, ISM, EPS

Flag Improves Terminal, Detection & Deactivation

MMSI, CMA Radio License, P&I, IS, WLC, WBC

CSR, ARPA, SPC, Special Qualification Licenses

VESSEL REGISTRATION COMPLETED

Ship Certificate of Registry issued
Set of Liberian Certificates and Publications onboard

(Liberian Registry, 2016)
Appendix 4: Ship Certificates Issued Electronically

Table provided on next page due to margins
<table>
<thead>
<tr>
<th>CERTIFICATE TITLES</th>
<th>Fitting Vessel over 500 GT</th>
<th>Fitting Vessel under 500 GT</th>
<th>Cargo Ship over 10000 GT</th>
<th>Cargo Ship under 10000 GT</th>
<th>Passenger Ship</th>
<th>Miscellaneous</th>
<th>Offshore</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Sewage Pollution Prevention Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM Safety Management Certificate (SOLAS)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM Safety Management Certificate (mezzanine L)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM Document of Compliance (SOLAS)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM Document of Compliance attachment (SOLAS)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMDG Code (SOLAS)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Tonnage Certificate (1989)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tonnage Certificate (small vessels)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tonnage Certificate (EU legislation)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-Government Certificate of Nationality</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Royal Danish Certificate of Nationality</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Passenger Ship Safety Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lr.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISM, ISPS, and OCOP</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Ship Security Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Ship Security Certificate (mezzanine L)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permit for carriage of passengers</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permit for carriage of passengers (mezzanine L)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passenger Ship Safety Certificate (mezzanine L)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High-Speed Craft Safety Certificate (2000)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record of Equipment for High-Speed Craft Safety Certificate (2000)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record of Construction and Equipment for Ships other than Oil</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Record of Construction and Equipment for Oil Tankers</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Load Line Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Load Line Exception Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dangerous Goods</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-Fouling System Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record of Anti-Fouling System</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Declaration on Anti-Fouling System</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passenger Ships</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>International Air Pollution Prevention Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>International Air Pollution Prevention Certificate (mezzanine L)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Certificate for the supplement to ISM Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Approval Certificate for the supplement to ISM Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Exemption Certificate (International Convention for the Safety of Life)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Safety for burden of pollution damage</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Safety for oil pollution damage</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>For the death of and personal injury to passengers</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Record of equipment for the certificate of compliance</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>National Record of Equipment for fishing vessels</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>National Cargo Ship Safety Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Form MI (Form MI)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>(Form MI)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>(Form MI)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Declaration in Danish waters</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Record of Equipment for the Cargo Ship Safety Certificate (Form C)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Cargo Ship Safety Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Cargo Ship Safety Route Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Stand-by Ship Permit</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Certificate of Approval of Live-stock Vessel</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Record of Equipment for the Cargo Ship Safety Certificate (Form C)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Intact Stability Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>GL Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Athenos Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Bunker Certificate</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

(VISMA Consulting a/s, 2017)
Appendix 5: ISA2 Reference Architecture for E-Documents

Source: European Commission ISA2 (JoinUp, 2016)
Appendix 6 : MA Press Releases and Maritime Announcements

BAHAMAS MARITIME AUTHORITY Information Bulletin 20180129

DNV-GL Electronic Class and Statutory Certificates

GOVERNMENT OF INDIA DIRECTORATE GENERAL OF SHIPPING E-cert announcement 20171218

IMO FAL.5/Circ.39/Rev.2 20 April 2016

KINGDOM OF DENMARK e-certificate announcement press release 20160620

MARITIME AND PORT AUTHORITY OF SINGAPORE electronic certificate announcement 20161130

PANAMA MARITIME AUTHORITY Merchant Marine Circular 20170830

PARIS MOU Guidelines on the use of electronic certificates

TRANSPORT MALTA Merchant Shipping Notice 20171026

82
## Appendix 7: Fleet Ownership & Registration, Main Economies, 2017

<table>
<thead>
<tr>
<th>Economy of ownership (Ranked by number of ships owned)</th>
<th>Flag of registration (Ranked by number of ships registered)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panama</td>
<td>China</td>
</tr>
<tr>
<td>China</td>
<td>559</td>
</tr>
<tr>
<td>Greece</td>
<td>420</td>
</tr>
<tr>
<td>Japan</td>
<td>2 225</td>
</tr>
<tr>
<td>Germany</td>
<td>29</td>
</tr>
<tr>
<td>Singapore</td>
<td>222</td>
</tr>
<tr>
<td>United States</td>
<td>99</td>
</tr>
<tr>
<td>Norway</td>
<td>55</td>
</tr>
<tr>
<td>Indonesia</td>
<td>21</td>
</tr>
<tr>
<td>Russian Fed’n</td>
<td>28</td>
</tr>
<tr>
<td>R. of Korea</td>
<td>534</td>
</tr>
<tr>
<td>World</td>
<td>6 543</td>
</tr>
</tbody>
</table>

Sources: UNCTAD (UNCTAD, 2017a); Clarksons Research. /Note: Commercial ships => of 1000 gt
Appendix 8  IMO RESOLUTION MSC.428(98)

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,
1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

Source: International Maritime Organization
MSC 98/23/Add.1 Annex 10, page 1
I:\MSC\98\MSC 98-23-Add-1.docx