UDC 656.6:004.738.5 DOI https://doi.org/10.33082/td.2026.2-29.02

CONCEPTUAL DISTRIBUTED INFORMATION SYSTEM MODEL FOR SHIP CERTIFICATES PROCESSING

D.O. Iakymenkov[1], O.I. Sagaydak[2]
[1]IMO expert, Postgraduate
Odesa National Maritime University, Odesa, Ukraine
ORCID ID: 0009-0001-1527-0236
[2]PhD, IMO expert, Senior Lecturer, Navigation and Ship's Handling Chair
Odesa National Maritime University, Odesa, Ukraine
ORCID ID: 0000-0002-8294-8828

Summary

Nowadays, there has been a significant increase in the speed of loading and discharging operations in ports, as well as in ship speeds at sea. This trend leads ship managers to attempt to reduce the time spent on non-commercial operations. Inspections carried out by Port State Control (PSC) or Flag State Control (FSC) are typical examples of such operations. Although these inspections do not generate profit, they are essential for ensuring maritime safety and therefore cannot be shortened without compromising safety.

However, certain procedures may be optimised through the application of modern information technologies. One such procedure is the verification of ship documents for authenticity.

***Purpose:** The purpose of this article is to propose a conceptual model for IT solution that facilitate the verification and validation of the ship documentation. The assessment includes the identification of the gaps, formalisation of the requirements based on the available enterprise architectures, and analysis of several of the most effective industry-standard technologies applicable to PSC and FSC procedures according to these requirements. These technologies were subsequently analysed in terms of their advantages and disadvantages, based on their implementation in various domains, as well as their adaptability to maritime procedures.*

***Results:** As a result of this research, the conceptual model of the IMO ship's certificate system is proposed. The study consistently and convincingly demonstrates the compliance of the proposed model with the formal criteria and satisfaction of the initial requirements for the formulated problem.*

***Conclusions:** Based on the findings, a new conceptual interaction model is proposed, based on the ePhyto system that is already implemented within certain United Nations agencies. This model is efficient, reliable, and requires minimal adaptation compared to alternative solutions. Given that the International Maritime Organization (IMO) is also a United Nations agency, this approach represents a cost-effective and practical solution for improving document verification procedures.*

***Key words:** IT technologies, port and flag state control, document check, ship inspection, ePhyto model, Maritime Transport, Safety, Containers, Cybersecurity, Decision-support systems, Operational Efficiency, Reliability, Optimization, Regulatory*

Compliance, Artificial Intelligence (AI), Cargo Handling, Fuzzy Logic, Intelligent systems, Logistics, Supply Chain Integration, Terminal management, Approximation model, Cost minimization, Information priority, Knowledge extraction, Marine logistics, Port operations, Process description, Professional development, Project management, Semantic classification, Standardization, Transport automation, User competence.

КОНЦЕПТУАЛЬНА МОДЕЛЬ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ОБРОБКИ СУДНОВИХ СЕРТИФІКАТІВ

Д. А. Якименков[1], О. І. Сагайдак[2]
[1]експерт ІМО, аспірант
Одеський національний морський університет, Одеса, Україна
ORCID ID: 0009-0001-1527-0236
[2]доктор філософії, експерт ІМО, ст. викладач кафедри НКС
Одеський національний морський університет, Одеса, Україна
ORCID ID: 0000-0002-8294-8828

Анотація

Вступ. *У наш час спостерігається значне збільшення швидкості вантажно-розвантажувальних операцій у портах, а також швидкості суден у морі. Ця тенденція змушує менеджерів суден намагатися скоротити час, витрачений на некомерційні операції. Типовими прикладами таких операцій є інспекції, що проводяться органами контролю держави порту (PSC) або контролю держави прапору (FSC). Хоча ці інспекції не приносять прибутку, вони важливі для забезпечення безпеки на морі, тому їх не можна скоротити без шкоди для безпеки.*

Проте деякі процедури можна оптимізувати за допомогою сучасних інформаційних технологій. Однією з таких процедур є перевірка суднових документів на справжність.

Мета: *мета цієї статті полягає в тому, щоб запропонувати концептуальну модель IT-рішення, яке полегшить перевірку та валідацію суднової документації. Оцінка включає виявлення прогалин, формалізацію вимог на основі наявних корпоративних архітектур та аналіз кількох найбільш ефективних галузевих стандартних технологій, застосовних до процедур PSC і FSC відповідно до цих вимог. Згодом ці технології були проаналізовані з точки зору їхніх переваг і недоліків на основі їх впровадження в різних областях, а також їх адаптованості до морських процедур.*

Результати: *в результаті цього дослідження запропоновано концептуальну модель системи суднових сертифікатів ІМО. Дослідження послідовно та переконливо демонструє відповідність запропонованої моделі формальним критеріям та відповідність вихідним вимогам до сформульованої проблеми.*

Висновки: *на основі отриманих даних запропоновано нову концептуальну модель взаємодії, засновану на системі ePhyto, яка вже впроваджена в деяких установах ООН. Ця модель є ефективною, надійною та потребує мінімальної адаптації порівняно з альтернативними рішеннями. З огляду на те, що Міжнародна морська організація (ІМО) також є установою ООН, цей підхід є економічно ефективним і практичним рішенням для вдосконалення процедур перевірки документів.*

 ISSN 2616-7360

Ключові слова: *IT технології, контроль держави порту та прапору, перевірка документів, інспекція судна, ePhyto модель, морський транспорт, безпека, контейнери, кібербезпека, системи підтримки рішень, операційна ефективність, надійність, оптимізація, відповідність вимогам, штучний інтелект (ШІ), обробка вантажів, нечітка логіка, розумні системи, логістика, інтеграція ланцюгів постачання, керування терміналом, модель апроксимації, мінімізація витрат, інформаційний пріоритет, вилучення знань, морська логістика, портові операції, опис процесу, професійний розвиток, управління проектами, семантична класифікація, стандартизація, автоматизація транспорту, компетенція користувача.*

Introduction

Modern shipping is characterised by high operational speeds and increasing vessel sizes. The number of ships has also grown significantly. The speed of port operations has increased considerably compared to a decade ago; loading and discharging operations that once took weeks may now be completed within hours. Consequently, the duration of cargo operations has become comparable to auxiliary ship operations such as mooring, bunkering, or obtaining free pratique.

In such circumstances, ship managers strive to minimise the duration of non-revenue-generating activities. At the same time, shortening certain operations may have serious implications for safety (e.g. mooring), while others remain mandatory for vessels calling at ports, such as inspections by PSC or FSC authorities.

According to the United Nations Convention on the Law of the Sea (UNCLOS), the Flag State bears primary responsibility for the safety of its vessels. This responsibility is exercised through periodic surveys and the issuance of certificates confirming compliance. Port States, in turn, are entitled and obliged to verify compliance with safety and environmental protection requirements during a vessel's port stay. [1].

Moreover, according to the Article 217 (3) of UNCLOS, Flag State must provide all crew members of the ship, flying its flag, with the certificates (licenses), for proving their competency.

Flag States may delegate certain responsibilities to Recognized Organizations (ROs), including surveys and certification activities (according to the RO Code – MSC.349(92) and MEPC.237(65)) [2]. In particular, Flag State can delegate to RO duties on fulfilling surveys of its ships and issuing proper certificates of compliance with the regulations.

Port State is to fulfil inspections on compliance monitoring (Article 219 of UNCLOS) [1]. According to Procedures for Port State Control, such inspections in general, to be limited by the inspection of documents, such as certificates of the ship, issued by Flag State and RO, and crew licenses and certificates, issued by National Authorities of the crew and endorsed by Flag State. More detailed inspection to be initiated in case clear grounds of non-compliance is found only [3].

In addition to regulatory inspections, vessels may also be inspected by commercial entities, such as charterers, particularly in the tanker sector. These inspections typically begin with document verification.

Thus, the accuracy and efficiency of document inspection are critical. Errors may result in undue delays or, conversely, failure to identify substandard vessels. Although inspections are often conducted in parallel with cargo operations, they impose additional workload on crew members, who are already operating under constrained conditions.

In general, survey or inspection of the ship should not affect ship's activity – cargo operations and other. However, even if inspection is carrying out in parallel with cargo

operations, ship's crew should be engaged in it anyway. Taking into account limited number of the crew members and their constant overload with the other tasks, inspection affects ship's activity in any case – it is additional workload for the crew.

It should be noticed the high importance of the timely inspection of the ship, which is essential part of the unified system of Compliance Monitoring and, on the other hand, can affect ship's operations. Therefore, improving the efficiency of document verification processes is significant for all stakeholders in the maritime industry.

This article will propose an assessment of the existing IT best practices that are present in logistics. To achieve this goal as a first step the requirements would be formulated. Then widely used enterprise architectures would be reviewed as a framework for such requirements application. And as a last step, some of the best IT solutions, that are close to the requirements, would be compared using the best matching enterprise architecture approach.

The purpose of this article is to propose a new conceptual model for interaction between parties involved in port and flag control procedures, based on an analysis and evaluation of best practices and approaches.

Current situation

At present, most ship and seafarer certificates are issued in paper form. Consequently, inspections can generally only be conducted once a vessel has arrived at port. Some administrations require scanned copies of certificates to be submitted in advance; however, this does not significantly accelerate verification.

As usual, Flag Administration issues just a few types of certificates (usually these are Flag Certificate, Radio Station Certificate and Minimum Safe Manning Certificate), all other certificates to be issued by Recognized Organization.

Certificates issued by Flag States can usually be verified via official administration websites. However, certificates issued by ROs are more difficult to verify due to the large number of organizations and lack of standardisation. (the certificates of the IACS members relatively straightforward to check for authenticity).

However, problem might appear even with IACS certificates – when the ship passed some survey in time, but original certificate still not delivered on board of the ship due to delay of the courier mail or some other reason. Absence of the certificate may lead to the detailed inspection.

Another problem – ships of so-called "shadow fleet" – quite large number of vessels that operate without full regulatory compliance, or ships used to circumvent sanctions, oversight, or certification requirements. It may also refer to vessels with hidden or non-disclosed flags, beneficial ownerships, or misrepresented registry details. The key risks include regulatory, safety, financial, and environmental dimensions.

There are many risks associated with the operation of a "shadow fleet":

Regulatory and compliance risks

– Operating without valid or recognized certificates, or under improper flag/RO authorization.

– Inadequate ISM audits, safety management, or crew training not aligned with flag/RO expectations.

– Sanctions and trade restrictions that make shadow fleet operations illegal or risky.

Safety and environmental risks

– Substandard safety management leading to higher likelihood of accidents, pollution, and crew harm.

– Inadequate maintenance and certification of safety-critical equipment (lifesaving appliances, firefighting, pollution prevention equipment).

– Higher risk of port state detentions, leading to operational delays, cargo losses, and reputational damage.

ISSN 2616-7360

Financial and operational risks

– Increased insurance premiums, non-coverage due to non-compliance, or difficulty obtaining P&I coverage.

– Higher likelihood of port state detentions, cargo rejection, lay-up costs, and scrapping liabilities.

– Revenue leakage and increased downtime due to lack of access to legitimate financing, charters, or insurance markets.

Reputation and sanctions risks

– Association with illicit registries or shadow fleet practices can trigger investigations, reputation harm, and loss of business.

– Difficulty in obtaining future charters or access to certain ports or markets.

Checking all documents of such ships (including insurance certificates / P&I documentation) gives the opportunity to find out substandard ship easily. But it is not so easy to do it quickly and carefully. Every ship must keep on board quite a large number of various certificates (see as example requirements of Panama flag – Table 1).

Table 1

Example of the ship's documents, required by Flag State (in particular – Panama)

PANAMA		
TYPE OF CERTIFICATE	**CONVENTION**	
Safety Construction Certificate	SOLAS 92 I/12(a)(ii)	X
Safety Equipment certificate	SOLAS 92 I/12(a)(iii)	X
Safety Radio certificate	SOLAS 92 I/12(a)(iv)	X
ILLC (66) (Intl. Load Line)	LOAD LINE 66 art. 16	X
IOPP certificate MARPOL	73/78 Annex I reg.5	X
NLS/IPPC certificate (*1)	MARPOL 73/78 Annex II reg.12, 12A	
ISPP certificate	MARPOL 73/78 Annex IV reg.4	X
ICOF / COF chem	IBC Code section 1.5 /BCH Code section 1.6	
ICOF / COF gas	IGC Code section 1.5 /GC Code and GC ex Code section 1.6	
ISM – (SMC) certificate	SOLAS 92 IX/4.3	X
ISM – (DOC) certificate	SOLAS 92 IX/4.1	X
Document of compliance (dangerous goods)	SOLAS 92 II-2/54.3	X
ILO crew accommodation	ILO 92 and 133	X
Cargo gear booklet	ILO 152 art. 25	X
ITC 69	ITC 1969 art. 7	X
Carriage of grain	SOLAS REG VI	X
BC Code Attestation Letter	BC CODE	X
ISPS (ISSC)	SOLAS Ch. XI-2	X
ISPS(SSP)	SOLAS Ch. XI-2	X
IAPP certificate	MARPOL 73/78 Annex VI Reg.6	X
EAPP certificate	MARPOL 73/78 Annex VI Reg. 5 & 6	X
Passenger Ship Safety Cert	SOLAS 92 I/12	

Exhaustive list of the certificates required could be found in the List of Certificates and Documents Required to be Carried on Board Ships, 2022) [4].

The situation with the documents of seafarers is also inadequate: there is a special webpage on the IMO website for this purpose. However, it is not database

of the documents, this page leads to the links to the websites of appropriate Maritime Administration. Each of them has own construction, structure and abilities, so check of the documents for authenticity can take quite long time. But it is necessary to do this, taking into account large number of fraudulent documents found every year [5, 6].

So, even if some of the scanned certificates is sent to PSC office in advance (to send all of them is technically difficult), it will take long time to check them (if the careful checking procedure is supposed). This labour-intensive task takes not the time only, but resources as well. Also – there is still a room for the human error and to the possibility to make fraud certificates.

Problem description

Paper-based certification presents several operational challenges. Sometimes, paper certificates cannot be issued immediately on completing survey (if they are to be issued in the head office of RO, for example). In such situation, ship manager has also to wait till certificate will be delivered by mail – it takes additional time. Another time required for delivering from ship manager's office to the ship. Meantime, absence of any certificate on board may be considered as clear ground for detailed inspection of the ship. Detailed inspection means additional workload for the ship's crew and possible nonconformities, even if the ship is in good condition. It is recognized by IMO [7].

Paper certificate could be damaged or lost – almost in all such cases detailed inspection could not be avoided and ship will have to wait till new certificate or duplicate will be delivered. Situation with the seafarer might be even worse: in the most cases duplicate of the License or Certificate of Competency could not be issued very quick, thus the best solution in such situation is to replace this crew member, which is challenging, if this is an officer (it is not so easy to find proper candidate, to arrange entry visa, book flight, etc.)

Significant part of documental inspection is checking the certificates for authenticity. Even when verification is performed, fraudulent documents may still be difficult to detect. Meantime, there is no common database of all seafarers' documents or unified system of the similar websites (each Maritime Administration develops system of documents' check under its possibilities and wishes). Therefore, Port State Control officer might face difficulties or even technical problems while fulfilling the procedure of checking documents.

Besides that, checking of the documents doesn't guarantee their authenticity because of many methods to fake them.

Last, but not least – paper documents need paper for issuing them and energy to print them out.

Nowadays International Maritime Organization allows to issue electronic certificates [7]. However, verification procedure still remains the same. IMO doesn't require any specific form or format of the electronic certificates, leaving it to national jurisdictions (electronic certificates must comply with cyber security requirements of the International Organization for Standardization/International Electrotechnical Commission 27000 series standards and similar guidelines). This is traditional IMO approach; however, absence of harmonized format and common requirements makes use of electronic certificates more complex and slow down verification process.

Definition of the Model

Port State Control (PSC) and Flag State Control (FSC) represent distinct regulatory frameworks with different legal bases, responsibilities, and access to information.

ISSN 2616-7360

FSC is responsible for certification and ongoing compliance monitoring, while PSC focuses on enforcement through inspections of foreign vessels.

The proposed model distinguishes clearly between these roles and ensures that access to information and authority is appropriately allocated.

Pic. 1. Interaction Model definition

Here's a concise, structured comparison between State Control (PSC) and Flag State Control (FSC) in the maritime domain, focusing on legal nature, functional differences, roles of entities, and levels of access to information.

According to the UNCLOS Convention [1] the main responsibility for the safety of the ship lies with Flag State Control, which can delegate some authority for survey and certification of the ship to Recognized Organization (RO). Functions of the Port State are to fulfil duties of compliance monitoring and enforcement (CME) and to implement appropriate regime of safety monitoring in the ports of the state.

1) Legal nature

FSC (Flag State Control)

– Legal basis: FSC is the exercise of the flag state's duties to ensure ships registered under its flag comply with international and national standards. This is a sovereign obligation of the flag state to verify proper certification, crewing, safety management, and conformity with applicable conventions.

– Relationship to international law: FSC is primarily the flag state's own regulatory oversight and enforcement. It uses domestic legislation aligned with international conventions and is guided by IMO instruments and, where applicable, regional regimes.

PSC (Port State Control)

– Legal basis: PSC is a regional or international framework that authorizes port states to inspect foreign ships calling at their ports to verify compliance with international maritime conventions and national regulations. It is rooted in international conventions (e.g., SOLAS, MARPOL, Load Lines, STCW) and, where applicable, regional MOUs (Memoranda of Understanding) on PSC.

– Relationship to international law: PSC activities are state-to-state enforcement actions exercised by a port state under its sovereign authority, supported by the ship's flag state obligations under international law.

2) Functional differences (purpose and focus):

FSC

– Purpose: To ensure that ships registered under the flag are maintained to international standards and that the flag state can certify ships as compliant, issue and renew certificates, and ensure proper crewing and safety management.

– Primary focus: The flag state's own fleet oversight, including ship surveys, certification (e.g., safety, pollution prevention conformity), auditing of ship management companies, and verification of flag state compliance through recognized organizations.

– Outcome: Issuance or withdrawal of certificates, detention-related actions

within the flag state's jurisdiction, sanctions against non-compliant owners/managers, and maintenance of the flag state's register's credibility.

PSC

– Purpose: To verify that ships calling at their ports comply with key international safety, security, and environmental protection standards; to identify deficiencies and, if necessary, detain or limit access to the port or cargo operations.

– Primary focus: Conditions aboard ships visiting the port, life-saving appliances, fire safety, machinery, crewing, documentation, and overall compliance with SOLAS, MARPOL, STCW, Load Lines, etc.

– Outcome: Issuance of deficiency lists/Detention decisions for substandard ships; inclusion in the MOU's PSC regime (IMOs listings) if deficiencies are serious; sunctions to substandard ships and potential sanctions in the ship's next port calls.

3) Roles of entities involved

FSC

– Key actors: Flag state competent authority (ROs), flag state inspectors, port state authorities may still coordinate but FSC decisions originate from the flag state. Flag state authorities may rely on classification societies (ROs) in audits of ship management companies, and on-board surveys.

– Data and information: Ship certificates, survey reports, crew certifications, ISM/ISPS, safety management system documentation, CG/Seafarers' records, corporate management systems, and shipyard/maintenance data. The flag state maintains the ship registry and historical compliance data.

PSC

– Key actors: Port state control authorities as the primary decision-maker is the port state. MOUs (e.g., Paris MOU, Tokyo MOU) provide harmonized procedures and information-sharing.

– Data and information: Ships' certificates, crew lists, safety manuals, maintenance records, and inspection results. Information is shared within the MOU network to identify non-compliant ships and to track a ship's PSC history.

4) Levels of access to information

FSC

– Accessibility: The flag state has access to all data related to its ships: certificates, surveys, crewing, and management. Access extends to internal registries, surveyor findings, and enforcement records. Limited sharing with other flag states or international bodies is possible when interoperable systems exist (e.g., ISM/ISPS verification and mutual recognition frameworks).

– Public visibility: Certification status and major disciplinary actions may be publicly available (e.g., via the flag state registry or IMO public records). Detailed internal audit results are typically confidential and used for regulatory actions within the flag state.

PSC

– Accessibility: Access is typically constrained to the ship under inspection and relevant port state authorities, plus any information shared via MOUs among port states for enforcement and risk assessment. The ship's inspection report becomes part of the ship's PSC history and can be shared with other port states under MOU procedures.

– Public visibility: Some PSC results (e.g., detention lists) may be publicly disclosed by MOUs or national authorities for transparency and to inform stakeholders. Detailed inspection reports are usually restricted to authorized authorities.

5) Interaction and dynamics – PSC and FSC interact indirectly but are distinct functions:

ISSN 2616-7360

– A ship may be FSC compliant (i.e., holds valid certificates from its flag state), yet fail a PSC inspection when visiting a port state, leading to detentions or remedial actions under the port state's procedures.

– Conversely, a ship flagged by a compliant flag state may still have PSC deficiencies when visiting another port, prompting the port state to take action independent of the flag state's ongoing oversight.

– PSC has the obligation to inform Flag Administration about detention of the ship and major deficiencies found. Flag State has to take remedy actions to close deficiencies found.

– Information sharing occurs through international networks (e.g., IMO instruments, Paris/Madrid MOUs) to enhance global safety and environmental protection by enabling cross-referencing of ship histories and risk profiles.

6) Practical implications for stakeholders

– Shipowners and operators

– Must maintain both flag state compliance (certificates, ISM/ISPS, crew qualifications) and readiness for PSC inspections in any port they call.

– Detentions under PSC can affect voyage schedules, insurance, and reputational risk; FSC non-compliance can lead to certificate withdrawal, increased regulatory scrutiny, and potential flag state sanctions.

– Port states and flag states

– PSC acts as a frontline enforcement tool in ports to ensure international standards are met by visiting ships; FSC acts as the ongoing regulatory oversight to keep the flag state register credible.

– Effective information systems and cooperation between PSC authorities and flag state competent authorities are essential to minimize duplication of work and ensure consistent enforcement.

Maritime industry has some certain specific in the issuing, verification and checking of the validity of the certificates. Major number of certificates are issued by Flag State or it's Recognized Organizations (FS delegates certain survey tasks to an RO under a formal MOA/authorization). ROs issue primary certificates on behalf of the FS (e.g., Safety Equipment Certificate, International Ship Security Certificate under the authority of the FS). The ship remains under the flag; the RO's survey reports are reviewed by the FS for final acceptance.

Issued marine certificates are subject for periodical updates and has some certain renewal cycles (typically certificates are typically valid for five years (subject to intermediate/annual surveys). ROs perform the on-board surveys, including annual/quarterly checks as mandated, but the exact cadence depends on the certificate type and flag state instructions.

Many ships operate under a "two-issuer" cadence at times: a certificate from the ROs (on behalf of the FS) and a separate statutory certificate still managed/resolved by the Flag State. Some information may be consolidated in a centralized national or regional system, but cross-checks with the FS/RO are routine.

There are several existing information systems:

– IMO DCS – the IMO ship fuel oil consumption system, consisting of requirements for ships to record and report their fuel oil consumption with a view to inform further IMO measures to reduce GHG emissions from ships.

– IHM (Inventory of Hazardous Materials) – assists compliance with regulation 5 of the Hong Kong International Convention for the Safe and Environmentally Sound Recycling of Ships, 2009

Besides that, there is several European information systems and systems of other international organizations. Integration to these information systems at the present moment seems to be not feasible due to increasing of system complexity and some other reasons, not connected to technical aspects. The feasibility of such integration to be reviewed at the next step of the research.

Thus, the only IMO system, which could be considered for the integration in this research is Global Integrated Shipping Information System (GISIS) – comprehensive online hub for the collection, processing and sharing of shipping-related data. It includes a wide range of modules, including those on: (i)contact points; (ii)global SAR plan; (iii) incidents of piracy; (iv)marine casualties; (v)ship and company particulars; and (vi) port reception facilities. IMO called for improvement of this system; thus our aim is to facilitate the work of it. Several aspects to be taken into account:

Data flows and typical integration points

– Flag States feed certificates, audit results, and ship registries into IMO database (GISIS) and national maritime administration portals.

– ROs submit survey reports and certificates to the FS and, where applicable, to IMO system (GISIS).

– shipowners/operators may access national or RO portals to obtain certificate statuses, due dates, and renewal requirements; port State Control may query GISIS and national systems for compliance.

Interoperability challenges

– Variability in data formats, certificate naming, and reporting standards across Flag States and ROs.

– Delays in updating status after surveys or renewals.

– Incomplete coverage for some ships, especially those in transitional status (e.g., newbuilds, re-flagging).

Practical implications

– For operators: need robust document management to track certificate validity, renewal windows, and RO/FS dependencies.

– For regulators and port controls: potential friction if data is not synchronized – risk of delays.

Mitigation strategy for the "shadow fleet"

– Maintain a single authoritative, auditable record of certificates, with clear ownership and expiry dates.

– Use unified document management system (GISIS would be the best suitable) that tracks RO issuance, FS approvals, and IMO submissions.

– Implement standardized data formats for certificates (e.g., use EDI or API-based integration with RO/FS portals and GISIS where available).

– Establish automated alerts for renewals, re-surveys, and status changes.

Such system will allow to vet flags, ownership chains, and RO/FS legitimacy before entering charters or leasing ships. As additional function – monitoring of sanctions lists, flag-state credibility, and RO accreditation status.

Purposes of the research: general tasks to be fulfilled

The high-level requirements for the system of world ships and crew's documents could be form like in the Table 2:

ISSN 2616-7360

Table 2

List of system requirements

ID	Requirement Description	Category	Priority	Rationale
RQ-01	System must provide easy access for users.	Accessibility & Usability	High	Ensures users can reach the system without obstacles.
RQ-02	System must offer a simple but secure authorization method.	Security	High	Balances usability and security to prevent unauthorized access.
RQ-03	System must support fast operation and responsiveness.	Performance	High	Improves user efficiency and experience.
RQ-04	System must allow concurrent processing of many documents.	Performance	High	Enables high throughput in document handling.
RQ-05	System must provide a user-friendly interface.	Accessibility & Usability	High	Reduces training needs and user errors.
RQ-06	System must store large volumes of data for an unlimited time.	Performance & Scalability	Medium	Ensures archival and historical access.
RQ-07	System must be accessible globally via the internet.	Accessibility	High	Enables remote and distributed work.
RQ-08	System must ensure strong protection against unauthorized access.	Security	High	Protects confidential data.
RQ-09	System must prevent alteration of already uploaded documents.	Security & Data Integrity	High	Ensures document integrity and legal compliance.
RQ-10	System must offer protection against cyber-attacks.	Security	High	Protects system from external threats.
RQ-11	System must include robust virus protection mechanisms.	Security	Medium	Minimizes malware risk from uploaded files.
RQ-12	System should require minimal operator interference for operation.	Usability & Efficiency	Medium	Increases automation and reduces human error.
RQ-13	System should be independent (self-contained, minimal external dependencies).	System Autonomy	Medium	Enhances resilience and control.
RQ-14	System must remain stable and operational during power failures (e.g., via backup systems).	Reliability	High	Ensures business continuity.
RQ-15	System should be separate from general internet tools/ platforms.	Security & Autonomy	Low	Reduces risk of dependency or cross-contamination.
RQ-16	Development must engage minimal resources.	Cost Efficiency	Medium	Controls development costs.
RQ-17	System must incur minimal operating costs.	Cost Efficiency	High	Ensures sustainability of the system.
RQ-18	System must require minimal maintenance.	Maintenance	Medium	Reduces ongoing support efforts and costs.

Possible solutions

To address such requirements, several international IT standards for the enterprise architecture were considered, including:

– The Open Group Architecture Framework (TOGAF 10) [9]

– ISO/IEC/IEEE 42010 – Systems and Software Architecture [10]

– SABSA – Security Architecture [11]

– NIST Enterprise Architecture Model [12]
– ArchiMate (Standard Modelling Language for EA) [13]
Coverage of the requirements is shown in the next table:

Table 3

Comparison table of the requirements coverage by EAs

Requirement Group	TOGAF	ISO 42010	SABSA	NIST EA	ArchiMate
Accessibility & Usability	Yes	Yes	Partial	Yes	Yes
Performance & Scalability	Yes	Yes	Partial	Yes	Yes
Security & Data Integrity	Yes	Partial	Yes	Yes	Yes
System Autonomy & Reliability	Yes	Yes	Yes	Yes	Yes
Cost Efficiency & Maintenance	Yes	Yes	Partial	Yes	Partial

The complete coverage of all listed requirements is supported by TOGAF 10 and NIST EA. Further TOGAF will be used as an open standard. The next table maps the 18 identified system requirements to the respective architecture domains defined in the TOGAF framework. TOGAF divides enterprise architecture into four main domains: Business, Application, Data, and Technology. This mapping supports structured solution development and ensures coverage of both functional and non-functional needs.

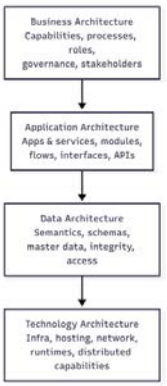
Table 4

Mapping of the system requirements to the TOGAF domains

Requirement	Description	TOGAF Domain(s)
RQ-01	Easy access	Application, Technology
RQ-02	Simple, but secure authorization method	Application, Security (cross-domain)
RQ-03	Fast operation	Application, Technology
RQ-04	Opportunity to process many documents at the same time	Application, Technology
RQ-05	User-friendly interface	Application
RQ-06	Possibility to keep huge volume of information for unlimited time	Data, Technology
RQ-07	Accessibility from any point of the world	Technology
RQ-08	Strong protection from unauthorized access	Security (cross-domain), Application
RQ-09	Strong protection from change of the document, already uploaded to the system	Data, Security (cross-domain)
RQ-10	Strong protection from cyber-attacks	Security (cross-domain), Technology
RQ-11	Maximum virus protection	Security (cross-domain), Technology
RQ-12	Minimal interference of operators	Business, Application
RQ-13	System to be independent	Technology
RQ-14	System to be stable and not dependent on possible power failure	Technology
RQ-15	System to be separate from other internet instruments	Technology, Security (cross-domain)
RQ-16	Minimal resources to be engaged for development	Business
RQ-17	Minimal operation costs to be involved	Business, Technology
RQ-18	Minimal maintenance to be required	Technology

The TOGAF system architecture can be represented as layered structure:

ISSN 2616-7360



Pic. 2. Diagram: TOGAF Architecture layers

To facilitate the analysis of possible IT solutions to cover the requirements for the system, that are listed before, the requirements could be grouped by these architecture layers. As a result, an exhaustive list of criteria for analysis is produced:

Table 5

Criteria derived from the TOGAF Architecture layers

TOGAF Layer	Definition	Derived Characteristics	Explanation	Why?
Business Architecture	Defines roles, responsibilities, business processes, governance, regulations	Local Independence	Each country defines and governs its own processes. System supports national procedures within a harmonized international model.	TOGAF separates business capabilities, enabling national autonomy within global exchange models.
		Decoupling (partial)	Business processes are modular and can be mapped to independent system components	
Application Architecture	Defines applications, components, services, APIs, workflows, and communication	Decoupling	Apps are designed as loosely coupled modules	TOGAF promotes service orientation and loose coupling for flexibility and autonomy.
		Interoperability	Defined service interfaces (e.g., XML messages, REST APIs) allow seamless interaction between national systems and the central hub.	
		Fault Tolerance (partial)	Retry mechanisms, stateless services, and message buffering allow the system to recover from transient failures.	
		Local Independence (reinforced)	National systems can be built using local platforms, as long as they respect global data exchange interface contracts.	

Continuation of table 5

TOGAF Layer	Definition	Derived Characteristics	Explanation	Why?
Data Architecture	Defines structure and semantics of information used across the system	Interoperability	Standardized schemas (e.g., UN/CEFACT SPS) ensure semantic alignment.	TOGAF advocates canonical data models and shared vocabularies to support integration.
		Security	Controlled access to data fields, validation of digital signatures, and ensuring document integrity rely on consistent data semantics.	
Technology Architecture	Defines infrastructure, hosting, networks, storage, and runtime environments	Distribution	Components are deployed in various regions – national servers, hubs, cloud services – and interact through secured networks.	TOGAF models physical and virtual infrastructure, emphasizing availability and performance.
		Scalability	Use of containerized services or cloud-native platforms allows the system to scale up/down based on demand (e.g., certificate surges).	
		Fault Tolerance	Failover mechanisms (e.g., backup queues, alternate hubs), retry logic, and monitoring ensure continuity of service.	
		Security (reinforced)	Network-level protections (firewalls, VPNs), endpoint hardening, and DDoS protection are implemented at infrastructure level.	
Security (Cross-layer)	Integrated across all layers to enforce trust, access control, and data protection	Security	Ensures authentication of actors, encryption of messages, validation of certificate signatures, and access control.	TOGAF and SABSA recommend embedding security architecture in all phases and layers.
		Fault Tolerance	Trust does not depend on the internal workings of other national solutions – only on message format and digital proof.	
		Decoupling	Ensures no data tampering during failover; fallback must be secure.	

Modern IT technologies propose several architecture templates for implementing such kind of IT system. Furter the best use-cases listed for the systems, used in logistics. These systems demonstrate examples of the best practices in highly distributed IT solutions, tailored for the digitalisation of the international trade and transport.

– UN IPPC ePhyto;

ISSN 2616-7360

– EU eFTI;
– Maersk/IBM Tradelens.

To formalise analysis of these systems, the 7 listed above criteria are to be used for comparation of each of these solutions and conclusions.

Analysis, general overview of the IT systems analysed

This review examines three representative initiatives: the UN IPPC ePhyto solution for phytosanitary certification, the EU electronic Freight Transport Information (eFTI) framework, and the blockchain-based TradeLens platform. Each provides insights into distributed architectures, data governance, and computational requirements in cross-border contexts.

1. UN IPPC ePhyto

The ePhyto certificate (ePhyto) [14] is the electronic version of the traditional paper phytosanitary certificate, ensuring that plant consignments comply with import standards. Its architecture is composed of national systems, the Generic ePhyto National System (GeNS) for countries lacking infrastructure, and the central ePhyto Hub, which routes and validates messages. Certificates are XML-based, conforming to the UN/CEFACT SPS data model, with mandatory security measures including encryption and digital signatures.

Governance is provided by the IPPC Secretariat with UN International Computing Centre (UNICC) [17] hosting the hub. The system enables developing countries to participate through GeNS while supporting integration with national Single Window environments. Benefits include reduced fraud, greater efficiency, and global interoperability with frameworks such as EU TRACES. Computationally, the ePhyto system emphasizes asynchronous communication, persistent queuing, and stateless endpoints to achieve scalability and resilience [18,19].

2. EU eFTI

The EU eFTI Regulation (EU) [23] 2020/1056 establishes a legal and technical framework for electronic communication of regulatory freight transport information. Its federated architecture [24] includes economic operators, certified eFTI platforms, eFTI gates for secure authority access, and national authorities as consumers. Data is decentralized and accessed through harmonized interfaces based on UN/CEFACT semantic models.

The system's design principles, derived from TOGAF methodology, emphasize data sovereignty, interoperability through open standards, trust, and scalability. Governance is coordinated by the European Commission through designated national authorities and certified platforms. eFTI aims to reduce administrative burden by enabling authorities to access once-only datasets across multimodal transport chains. The architecture relies on service-based integration, federated infrastructure, and robust identity management mechanisms, ensuring computational efficiency while accommodating diverse stakeholders.

3. TradeLens

TradeLens[26], developed by IBM and Maersk, illustrates the potential and challenges of blockchain in logistics. Although decommissioned in 2023, it remains a valuable case study. Built on Hyperledger Fabric, TradeLens provided a permissioned blockchain [27] where carriers, ports, customs, and shippers shared trusted data through cryptographic

verification and smart contracts. Events and documents such as bills of lading were stored on the distributed ledger, ensuring immutability and auditability.

The architecture mapped naturally to TOGAF layers: decentralized infrastructure for distribution and fault tolerance, smart contracts and APIs for decoupling, and standardized data models for interoperability. Governance was consortium-based, with participants operating their own blockchain nodes. Computationally, TradeLens demonstrated the benefits of distributed trust and resilience, though it faced adoption and governance challenges that limited sustainability.

Research

Mapping of the IT systems characteristics

The three solutions represent distinct but converging approaches to global data exchange. ePhyto emphasizes centralized coordination with distributed participation, ensuring interoperability and scalability through XML messaging and stateless design. eFTI promotes a federated model anchored in EU regulations, focusing on data sovereignty, semantic consistency, and governance aligned with policy frameworks. TradeLens demonstrates a blockchain-based trust infrastructure, offering immutability and resilience but with high governance and adoption complexity.

From a computational perspective, all solutions address key qualities: distribution, decoupling, interoperability, security, scalability, fault tolerance, and sovereignty. ePhyto achieves these through message queues and hub-based validation, eFTI through federated platforms and harmonized standards, and TradeLens through blockchain consensus and cryptographic identities. Each provides lessons for future systems balancing efficiency, inclusivity, and trust.

Table 6

Mapping of the IT systems characteristics

Topic	ePhyto (IPPC)	eFTI (EU)	TradeLens (IBM/Maersk)
Architecture of the System	Central hub with national systems and GeNS for inclusivity	Federated platforms, gates, and authorities	Permissioned blockchain (Hyperledger Fabric)
Architecture Component Roles and Descriptions	NPPOs manage national systems; UNICC runs hub; GeNS supports small states	Operators (data providers), platforms (hosts), gates (access points), authorities (consumers)	Shippers, ports, customs, and operators each run blockchain nodes
How the System Works	Certificates generated, validated, transmitted via hub	Data stored on eFTI platform; accessed by authorities via gates	Events/documents recorded on blockchain; accessed via smart contracts
Data Model	XML certificates, UN/CEFACT SPS model	Semantic models based on UN/CEFACT CCL	UN/CEFACT, GS1, WCO, EPCIS event models
System Requirements	Security, digital signatures, traceability, compliance with ISPM	Trust, data sovereignty, interoperability, eIDAS integration	Distributed trust, smart contracts, audit logs, cryptographic verification
Governance and Integration	Governed by IPPC Secretariat; integration with Single Windows	EU Commission coordination; national certification of platforms	Consortium governance (IBM, Maersk); integration via APIs or nodes
Benefits and Global Interoperability	Fraud reduction, developing country inclusion, WTO-SPS compliance	Reduced burden, harmonized access, multimodal interoperability	Trusted data sharing, immutability, cross-border compliance

ISSN 2616-7360

Options analysis

This comparison highlights the differences and similarities between the ePhyto, eFTI and Tradelens system architectures, based on the enterprise architecture characteristics formulated above. The main focus is on the systemic benefits, global interoperability, and dominant data flow directions between Economic Operators (EOs) and Authorities.

1. Comparative Analysis of Benefits and Interoperability

Table 7

Comparative analysis of benefits and interoperability

Characteristic	ePhyto	eFTI	TradeLens	Comparison Insight
Distribution	Hub + NPPO national systems	Federated EU platforms per MS	Decentralized ledger with global node network	TradeLens and ePhyto emphasize global coverage; eFTI is EU-specific.
Decoupling	Loose coupling via hub & XML	Certified APIs with metadata exchange	Smart contracts and channelized event flow	All systems enforce modularity; TradeLens achieves highest technical decoupling.
Interoperability	UN/CEFACT SPS CCL	UN/CEFACT + EU profiles	CEFACT, GS1 EPCIS, WCO	All leverage international models; TradeLens has broader event semantics.
Security	XML Signature and PKI	Access control via certified Gates	Ledger immutability, ACLs, smart contracts	eFTI and TradeLens have platform-level access; ePhyto uses document-level trust.
Scalability	Global hub access	Expandable with national gate deployments	Add new blockchain nodes	TradeLens is designed for global horizontal scale; eFTI is more localized.
Fault Tolerance	Hub fallback, retry mechanisms	Queueing and status sync	Multi-node consensus and replication	TradeLens is more fault-tolerant due to blockchain architecture.
Local Independence	Full NPPO autonomy	Member States operate platforms	Each stakeholder operates independent node	All support local control; TradeLens provides strong node autonomy.

2. Dominant Data Flow Patterns

Below is a comparison of the main data flow direction between Economic Operators (EOs) and Authorities:

Table 8

Dominant data flow pattern

System	Main Flow Direction	Flow Trigger	Implication
ePhyto	Push by NPPO to Hub, Pull by importer NPPO	Issuance of certificate	Data is proactively shared via a central hub
eFTI	Pull by authority using dataset reference	Inspection or customs control	EO gives access token; authority pulls when needed
TradeLens	Push from event originator, pull by subscribers	Supply chain events	Real-time decentralized event publication

This analysis shows that while ePhyto and eFTI are primarily regulatory reporting tools, TradeLens also covers supply chain event streaming. Each system demonstrates a different level of distribution, autonomy, and interoperability.

The ePhyto model supports proactive data sharing and centralized availability via a global hub, suitable for pre-declaration and coordination. In contrast, eFTI operates on demand with access managed by dataset references, suitable for regulatory access control and reducing data exposure. Tradelens is focused on operational B2B integration, while it was intended to work with real-time events, high delays of the underlying blockchain infrastructure makes this critical. The complexity of the blockchain together with its high latency limits the use of such kind of solution.

Adaptation of the ePhyto system to the conceptual model

Considering the distinguishing the roles of the PSC and FSC based on their legal nature, goals, subjects of control, levels of access to information and legal consequences of decisions made, it is important to highlight that the proposed Model supports two clearly demarcated operating modes:

– the Port State Control mode, which provides read-only access to validated certificate data for the purpose of inspection;

– the Flag State Control mode, which provides the issuing and surveillance authorities with the ability to manage the life cycle of certificates.

The roles of the PSC and FSC are clearly mapped to the matching roles in the ePhyto system:

Table 9

Mapping the roles within Models

PSC/FSC	Roles in Maritime Model	Roles in ePhyto model
	Central IMO Exchange Hub (CIeH)	Central ePhyto Hub (CeH)
FSC / RO	National certification organizations (NCO)	National Plant Protection Organization (NPPO)
Port State Control	Certificates consumers	Certificates consumers

Following the approach, proposed by the ePhyto, the NCO can use own IT solution (National System – NS) to connect to the CIeH, or utilize the Generic Vessels' Certificates National System (GeNS), that should provide minimum valuable functionality for the countries, that have no NS.

Such separation of the roles clearly shows that the proposed architecture discloses differences in user roles, access levels and legal consequences of relevant actions:

– does not grant PSC authorities the powers inherent in the FSC;

– makes it impossible to "mix roles" between the port state, the flag state and recognized organizations (ROs).

It is important to mention here, that proposed Model is fits perfectly the maritime certificates, taking into account the specifics of maritime transport, in particular:

– the dynamics of port calls (port call timeline);

– a significant number of certificates and a plurality of issuers (Flag State, RO);

– high criticality of vessel delays;

– risks associated with document falsification, particularly among vessels operating within the so-called "shadow fleet".

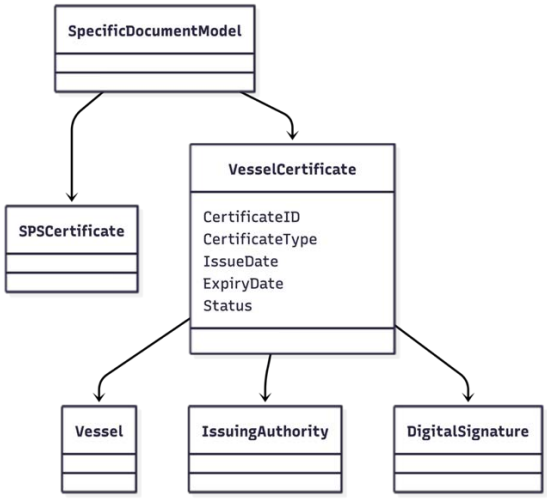
All these items have the same valuable roles in the plant protection workflow and are successfully implemented in the ePhyto model based on the UNICC computing resources.

ISSN 2616-7360

Extending the Interaction Model (Figure 1), the business components roles are also derived from the ePhyto system. They are:

– central IMO Exchange Hub,
– national certification organizations – NCO (NPPOs in ePhyto model):
– the Generic Vessels' Certificates National System (GeNS),
– national systems for countries with IT capabilities.
– certificates consumers – Port State Control

Adaptation of the ePhyto system for the vessel certificates purpose should also include data model of the certificate extension to support the vessel's certificates. Due the ePhyto data model is based on the UN/CEFACT data models hierarchy, that is also used for the IMO data modelling, particularly, IMO FAL Compendium, such extension is feasible.



Pic. 3 Vessel Certificate Data Model

Detailed adaptation plan is subject for development as a separate project, that should also cover the functional and technical requirements of the IMO IT infrastructure landscape.

Conclusions

The analysis of the reviewed solutions, that represent best practices for global trusted IT systems in logistics, demonstrates the feasibility of the IMO maritime certificates extension concept. IMO commenced major revision of the existing GISIS system. Some steps are made already on this way, mainly on interface and data visualization.

This article proposes a trustworthy enterprise architecture model for interaction between parties involved in port and flag state control procedures which provides a solution capable of offering quite seamless and reliable access to the marine certificates, that meets all major requirements and adds value to the efforts already done [28]. The formal assessment on the criteria, derived from the enterprise level architecture demonstrates advantages of the UN IPPC ePhyto solution as a reference implementation for this purpose. Still the proposed conceptual model requires some adaptation for

the specific requirements of the IMO and the task scope, the key advantage is operational trusted distributed architecture, that is based on clear requirements and data format. All components of this architecture (requirements, data model, deployment landscape for the central hub) are managed by UN body. Given its compatibility with existing UN frameworks, this approach represents a practical and scalable solution for the future development of maritime information systems. Considering that IMO is affiliated with UN, this approach can be scaled to IMO, including data model and system architecture.

REFERENCES

1. United Nations Convention on the Law of the Sea (UNCLOS-82). https://www.un.org/Depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm
2. RESOLUTION MSC.349(92) (Adopted on 21 June 2013) CODE FOR RECOGNIZED ORGANIZATIONS (RO CODE), IMO 2013
3. PROCEDURES FOR PORT STATE CONTROL, 2023 IMO Resolution A.1185(33) Adopted on 6 December 2023
4. LIST OF CERTIFICATES AND DOCUMENTS REQUIRED TO BE CARRIED ON BOARD SHIPS, IMO 2022 – FAL.2/Circ.133 MEPC.1/Circ.902 MSC.1/Circ.1646 LEG.2/Circ.4, IMO, 27 June 2022
5. REPORTS ON UNLAWFUL PRACTICES ASSOCIATED WITH CERTIFICATES OF COMPETENCY Report on fraudulent certificates. IMO HTW 9/INF.2
6. REPORTS ON UNLAWFUL PRACTICES ASSOCIATED WITH CERTIFICATES OF COMPETENCY Report on fraudulent certificates. IMO HTW 10/INF.2
7. GUIDELINES FOR THE USE OF ELECTRONIC CERTIFICATES FAL.5/Circ.39/Rev.2, IMO, 20 April 2016
8. Мазуренко О. К. Технології Blockchain в інформаційному забезпеченні логістичних послуг. *БІЗНЕСІНФОРМ.* 2019. № 12. С. 255 – 261.
9. The Open Group Architecture Framework (TOGAF 10) https://www.opengroup.org/togaf
10. ISO/IEC/IEEE 42010 – Systems and Software Architecture https://www.iso.org/standard/50508.html
11. SABSA – Security Architecture https://sabsa.org/
12. NIST Enterprise Architecture Model https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-167.pdf
13. ArchiMate (Standard Modeling Language for EA) https://pubs.opengroup.org/architecture/archimate32-doc/
14. IPPC: https://www.ippc.int
15. IISPM 7 (Phytosanitary certification system) https://www.ippc.int/en/publications/613/
16. ISPM 12 (Phytosanitary certificates) https://www.ippc.int/en/publications/609/
17. UNICC: https://www.unicc.org/news/2022/03/15/ippc-ephyto-solution-four-years-in
18. FAO Phytosanitary Certification Guidelines: https://www.fao.org/4/y3241e/y3241e06.htm
19. Grainmart: https://www.grainmart.in/news/procedure-for-inspection-and-issue-of-phytosanitary-certificate-psc

ISSN 2616-7360

20. Food Safety Works: https://foodsafetyworks.com/insights/phytosanitary-certificate-an-important-document-for-global-trade
21. Trade Facilitation: https://www.tradefacilitation.org/project/digitalising-processes-to-streamline-agricultural-trade
22. GENS IMPLEMENTATION FRAMEWORK, Version 1.0, 26 January 2021 Source: https://www.ephytoexchange.org/landing/assets/docs/ePhyto_GeNS_Implementation_Framework.pdf
23. Regulation (EU) 2020/1056 on electronic freight transport information (eFTI) https://eur-lex.europa.eu/eli/reg/2020/1056/oj/eng
24. eFTI Functional and Technical Architecture, European Commission, DG MOVE https://transport.ec.europa.eu/transport-themes/logistics-and-multimodal-transport/efti-regulation_en
25. EU DTLF Subgroup Reports and Recommendations https://transport.ec.europa.eu/transport-themes/digital-transport-and-logistics-forum-dtlf_en
26. IBM Blockchain and Maersk TradeLens Solution Overview https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens
27. Jensen, T., Hedman, J., & Henningsson, S. (2019). How TradeLens Delivers Business Value With Blockchain Technology. MIS Quarterly Executive, 18(4), 221-243. DOI:10.17705/2msqe.00018, https://www.researchgate.net/publication/345356583_How_TradeLens_Delivers_Business_Value_With_Blockchain_Technology
28. ENHANCEMENT OF GISIS. Update on the Global Integrated Shipping Information System (GISIS) review. C 134/9 17 May 2025, IMO London

ЛІТЕРАТУРА

1. United Nations Convention on the Law of the Sea (UNCLOS-82). https://www.un.org/Depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm
2. RESOLUTION MSC.349(92) (Adopted on 21 June 2013) CODE FOR RECOGNIZED ORGANIZATIONS (RO CODE), IMO 2013
3. PROCEDURES FOR PORT STATE CONTROL, 2023 IMO Resolution A.1185(33) Adopted on 6 December 2023
4. LIST OF CERTIFICATES AND DOCUMENTS REQUIRED TO BE CARRIED ON BOARD SHIPS, IMO 2022 – FAL.2/Circ.133 MEPC.1/Circ.902 MSC.1/Circ.1646 LEG.2/Circ.4, IMO, 27 June 2022
5. REPORTS ON UNLAWFUL PRACTICES ASSOCIATED WITH CERTIFICATES OF COMPETENCY Report on fraudulent certificates. IMO HTW 9/INF.2
6. REPORTS ON UNLAWFUL PRACTICES ASSOCIATED WITH CERTIFICATES OF COMPETENCY Report on fraudulent certificates. IMO HTW 10/INF.2
7. GUIDELINES FOR THE USE OF ELECTRONIC CERTIFICATES FAL.5/Circ.39/Rev.2, IMO, 20 April 2016
8. Мазуренко О. К. Технології Blockchain в інформаційному забезпеченні логістичних послуг. [Tekhnolohii Blockchain v informatsiinomu zabezpechenni lohistychnykh posluh] *БІЗНЕСІНФОРМ.* 2019. № 12. С. 255 – 261.
9. The Open Group Architecture Framework (TOGAF 10) https://www.opengroup.org/togaf

10. ISO/IEC/IEEE 42010 – Systems and Software Architecture https://www.iso.org/standard/50508.html
11. SABSA – Security Architecture https://sabsa.org/
12. NIST Enterprise Architecture Model https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-167.pdf
13. ArchiMate (Standard Modeling Language for EA) https://pubs.opengroup.org/architecture/archimate32-doc/
14. IPPC: https://www.ippc.int
15. IISPM 7 (Phytosanitary certification system) https://www.ippc.int/en/publications/613/
16. ISPM 12 (Phytosanitary certificates) https://www.ippc.int/en/publications/609/
17. UNICC: https://www.unicc.org/news/2022/03/15/ippc-ephyto-solution-four-years-in
18. FAO Phytosanitary Certification Guidelines: https://www.fao.org/4/y3241e/y3241e06.htm
19. Grainmart: https://www.grainmart.in/news/procedure-for-inspection-and-issue-of-phytosanitary-certificate-psc
20. Food Safety Works: https://foodsafetyworks.com/insights/phytosanitary-certificate-an-important-document-for-global-trade
21. Trade Facilitation: https://www.tradefacilitation.org/project/digitalising-processes-to-streamline-agricultural-trade
22. GENS IMPLEMENTATION FRAMEWORK, Version 1.0, 26 January 2021 Source: https://www.ephytoexchange.org/landing/assets/docs/ePhyto_GeNS_Implementation_Framework.pdf
23. Regulation (EU) 2020/1056 on electronic freight transport information (eFTI) https://eur-lex.europa.eu/eli/reg/2020/1056/oj/eng
24. eFTI Functional and Technical Architecture, European Commission, DG MOVE https://transport.ec.europa.eu/transport-themes/logistics-and-multimodal-transport/efti-regulation_en
25. EU DTLF Subgroup Reports and Recommendations https://transport.ec.europa.eu/transport-themes/digital-transport-and-logistics-forum-dtlf_en
26. IBM Blockchain and Maersk TradeLens Solution Overview https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens
27. Jensen, T., Hedman, J., & Henningsson, S. (2019). How TradeLens Delivers Business Value With Blockchain Technology. MIS Quarterly Executive, 18(4), 221-243. DOI:10.17705/2msqe.00018, https://www.researchgate.net/publication/345356583_How_TradeLens_Delivers_Business_Value_With_Blockchain_Technology
28. ENHANCEMENT OF GISIS. Update on the Global Integrated Shipping Information System (GISIS) review. C 134/9 17 May 2025, IMO London

Дата першого надходження статті до видання: 14.04.2026
Дата прийняття статті до друку після рецензування: 15.05.2026
Дата публікації (оприлюднення) статті: 01.07.2026