

AN AUTHENTICATION METHOD AND SYSTEM FOR MARITIME OPERATIONS

TECHNICAL FIELD

5

[001] The present specification relates broadly, but not exclusively, to an authentication method and system for maritime operations.

10 BACKGROUND OF THE DISCLOSURE

[002] Maritime operations typically rely heavily on fragmented, paper-based processes for identity authentication, document signing, port clearance, etc. Vessel identity information is often maintained in isolated databases across different jurisdictions, which may make real-time authentication and cross-port consistency difficult. In addition, each port that a vessel enters may need to re-validate the vessel and crew credentials from scratch, which may lead to duplication of effort and operational delays.

20 [003] Further, manual workflows involving physical ship stamps, wet ink signatures, and repeated data entry may not only reduce efficiency but may also introduce risks of fraud, miscommunication, and non-compliance.

[004] Typical frameworks used in maritime operations may not allow trusted interactions between vessels, ports, and regulatory boards. Hence, the typical frameworks may impede digital transformation in the maritime sector.

[005] A need therefore exists to provide an authentication method and system for maritime operations that seek to address at least some of the above problems. Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

35 SUMMARY

[006] According to a first aspect, there is provided an authentication method for maritime operations, comprising: validating, using an Identity Authentication system, Pre-Arrival Notification (PAN) vessel identity information based on a latest version of a vessel information record stored in a Ship Information Database, wherein: the vessel information record comprises validated vessel identity information; and the vessel identity information is validated based on government and/or regulatory boards databases; generating, upon validation of the PAN vessel identity information and using the Identity Authentication system, a machine-readable code, wherein: the machine-readable code embeds the latest version of the vessel information record and an authentication code; the embedded latest version of the vessel information record and authentication code are valid for a pre-determined period of time; and the authentication code comprises a random salt; and authenticating, using the Identity Authentication system, a vessel based on the generated machine-readable code and the Ship Information Database.

[007] According to a second aspect, there is provided an authentication system for maritime operations, comprising: an Identity Authentication system configured to: validate Pre-Arrival Notification (PAN) vessel identity information based on a latest version of a vessel information record stored in a Ship Information Database, wherein: the vessel information record comprises validated vessel identity information; and the vessel identity information is validated based on government and/or regulatory boards databases; generate, upon validation of the PAN vessel identity information, a machine-readable code, wherein: the machine-readable code embeds the latest version of the vessel information record and an authentication code; the embedded latest version of the vessel information record and authentication code are valid for a pre-determined period of time; and the authentication code comprises a random salt; and authenticate a vessel based on the generated machine-readable code and the Ship Information Database.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] Embodiments are provided by way of example only, and will be better understood and readily apparent to one of ordinary skill in the art from the following written description, read in conjunction with the drawings, in which:

[009] Figure 1 is a flowchart illustrating an authentication method for maritime operations, according to an example embodiment.

5 [0010] Figure 2 is a flowchart illustrating a port clearance process, according to an example embodiment.

[0011] Figure 3 is a flowchart illustrating a port departure process, according to an example embodiment.

10 [0012] Figure 4 is a schematic representation illustrating a vessel entering different ports, according to an example embodiment.

[0013] Figure 5 is a schematic representation illustrating a session termination process, according to an example embodiment.

15 [0014] Figure 6 is a flowchart illustrating an authentication code generation, according to an example embodiment.

20 [0015] Figure 7 is a schematic representation illustrating information embedded in a real-time QR code, according to an example embodiment.

[0016] Figure 8 is a flowchart illustrating an electronic document signing process, according to an example embodiment.

25 [0017] Figure 9 is an image of a digital stamp, according to an example embodiment.

[0018] Figure 10 is a flowchart illustrating an offline electronic document signing process, according to an example embodiment.

30 [0019] Figure 11 is a flowchart illustrating a document signing process for electronic bunker delivery notes (eBDNs), according to an example embodiment.

[0020] Figure 12 is a flowchart illustrating a document signing process for eBDNs, according to another example embodiment.

35 [0021] Figure 13 is an example image of an eBDN of Figure 11 and/or 12.

[0022] Figure 14 is a schematic diagram of a computer system suitable for use in executing at least some steps of the authentication method for maritime operations.

40

[0023] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

DETAILED DESCRIPTION

[0024] Embodiments will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0025] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0026] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as "scanning", "calculating", "determining", "replacing", "generating", "initializing", "outputting", or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0027] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other

apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a conventional computer will appear from the description below.

5 [0028] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language
10 and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or
15 scope of the invention.

[0029] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include
20 storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM, GPRS, 3G or 4G mobile telephone systems, as well as other wireless systems such as Bluetooth, ZigBee, Wi-Fi. The
25 computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0030] The present invention may also be implemented as hardware modules. More particularly, in the hardware sense, a module is a functional hardware unit designed for
30 use with other components or modules. For example, a module may be implemented using discrete electronic components, or it can form a portion of an entire electronic circuit such as an Application Specific Integrated Circuit (ASIC) or Field Programmable Gate Array (FPGA). Numerous other possibilities exist. Those skilled in the art will appreciate that the system can also be implemented as a combination of hardware and
35 software modules.

[0031] In the following description, the term “module” can refer to software, a hardware element, or a combination of both.

5 [0032] An Application Programming Interface (API) enables software and applications to communicate with each other. It is a software-to-software interface that allows for separate parties to communicate with each other without any previous user knowledge or intervention. In general terms, it is a set of clearly defined methods of communication between various software components.

10 [0033] This specification uses the term “configured to” in connection with systems, apparatus, and computer program components. For a system of one or more computers to be configured to perform particular operations or actions means that the system has installed on its software, firmware, hardware, or a combination of them that in operation cause the system to perform the operations or actions. For one or more
15 computer programs to be configured to perform particular operations or actions means that the one or more programs include instructions that, when executed by data processing apparatus, cause the apparatus to perform the operations or actions. For special-purpose logic circuitry to be configured to perform particular operations or actions means that the circuitry has electronic logic that performs the operations or
20 actions.

[0034] As used herein, the term “processing device” refers to any hardware or system configured to perform computational tasks.

25 [0035] Figure 1 is a flowchart 100 illustrating an authentication method for maritime operations, according to an example embodiment. At step 102, Pre-Arrival Notification (PAN) vessel identity information is validated using an Identity Authentication system based on a latest version of a vessel information record stored in a Ship Information Database. The vessel information record comprises validated vessel identity
30 information and the vessel identity information is validated based on government and/or regulatory boards databases. At step 104, a machine-readable code is generated using the Identity Authentication system upon validation of the PAN vessel identity information. The machine-readable code embeds the latest version of the vessel information record and an authentication code. The embedded latest version of
35 the vessel information record and authentication code are valid for a pre-determined period of time. The authentication code comprises a random salt. At step 106, a vessel is authenticated using the Identity Authentication system based on the generated

machine-readable code and the Ship Information Database. In the rest of this specification, the Identity Authentication system can be referred to as a Digital Identity Service Provider System.

5 **[0036]** As would be explained later, the authentication method advantageously improves operational integrity and operational efficiency, improves compliance, reduces fraud, and enhances cross-port interoperability across jurisdictions and port authorities for maritime stakeholders.

10 Vessel Identity Architecture and Federated Port Synchronization

[0037] A federated identity infrastructure, referred to as a Ship Information Database, may be leveraged as an authoritative source of vessel identity for maritime operations such as digital authentication and signing operations. The Ship Information Database
15 may act as a trusted registry of vessel data, structured for both sovereign hosting by individual countries and global interoperability through cryptographic standardization. The Ship Information Database can enable sovereign control by each participating jurisdiction while allowing synchronized, version-controlled identity sharing across ports.

20 *Verifiable Source*

[0038] Each vessel can be assigned a unique digital identity profile sourced from government or regulatory databases. The digital identity profile can include:

- 25 • International Maritime Organization (IMO) number
 • Digital Identity Service Provider number
 • Local vessel registration number
 • Flag state, ownership, technical details

The digital identity profile can be validated at the time of Pre-Arrival Notification (PAN)
30 and stored in the Ship Information Database as the vessel's current authoritative identity.

Consent-Driven Identity Sharing Workflow

35 **[0039]** According to one embodiment, the authentication method for maritime operations further comprises obtaining an authorization message from an authorized

device associated with the vessel using the Identity Authentication system, to transmit the latest version of the vessel information record to a selected port system before validating the PAN vessel identity information based on the latest version of the vessel information record stored in the Ship Information Database. The authorization message
5 from the authorized device associated with the vessel can be an approval to log in to an application from a device of an authorized personnel of the vessel. An example of the authorized personnel of the vessel can be a vessel master.

[0040] Figure 2 is a flowchart 200 illustrating a port clearance process, according to an
10 example embodiment. During port clearance, a consent-based mechanism may be triggered for an authorized personnel of the vessel to authorize use and sharing of the vessel's identity profile or vessel identity information. The Identity Authentication system or the Digital Identity Service Provider System may comprise a Digital Identity Service Provider Application. As shown in Figure 2, the vessel master can log in to a
15 third party service such as a Port Clearance Platform using the Digital Identity Service Provider Application and approve the log in using the Digital Identity Service Provider Application, in order to authorize use and sharing of the vessel's identity profile or vessel identity information for authentication purposes. Upon receipt of the authorization, the Ship Information Database may transmit the latest version of the
20 vessel information record or the vessel's identity with destination port's digital system(s) such as a Port Authority Platform. The Digital Identity Service Provider System may compare a PAN-submitted data against the stored latest version of the vessel information record or the vessel's identity in the Ship Information Database and/or government database(s). Upon successful validation or authentication, an
25 identity token may be issued and transmitted to the port's digital system to enable synchronized retrieval and verification of a current identity version of the vessel. Advantageously, this mechanism enables trusted identity continuity while allowing each country or port to maintain control over its registry and validation logic.

[0041] Figure 3 is a flowchart 300 illustrating a port departure process, according to an
30 example embodiment. Similar to the port clearance process described above, the consent-based mechanism may be triggered. As shown in Figure 3, the vessel master or an agent can log in to the port's digital system(s) such as the Port Authority Platform and approve the log in using the Digital Identity Service Provider Application. Summary
35 data of the vessel comprising information of the vessel's stay at the port may be stored by the Digital Identity Service Provider Application.

Version-Control

5 [0042] According to one embodiment, the authentication method for maritime operations further comprises applying version control to the vessel information record stored in the Ship Information Database using the Identity Authentication system.

10 [0043] Figure 4 is a schematic representation 400 illustrating a vessel entering different ports, according to an example embodiment. Each identity profile or vessel information record in the Ship Information Database may be version-controlled to track historical changes. This advantageously maintains data integrity throughout the vessel's voyage.

15 [0044] As shown in Figure 4, upon arrival at Port A, the vessel may submit PAN and provide consent to share its vessel identity information. Port A may validate the vessel identity information using government database(s). Thereafter, a vessel information record named for example, Ship Info V1, may be generated and stored in Port A's Ship Information Database.

20 [0045] Upon proceeding to Port B, the vessel may submit PAN and provide consent to share its vessel identity information again. Port B's Ship Information Database may request the latest version of the vessel information record (i.e. the Ship Info V1) from Port A. Any changes to the PAN (e.g., name, flag, crew, ownership) may be verified. Thereafter, a new vessel information record named for example, Ship Info V2, may be
25 generated. The new vessel information record (e.g., Ship Info V2) may become a current valid profile.

30 [0046] As the vessel transits between ports (e.g., Port A to Port B then to Port C), the authentication method for maritime operations advantageously ensures automatic synchronization of vessel identity records or vessel information records based on a vessel's last verified version of the vessel information record, updates submitted during PAN or through official channels and cryptographic hashing to allow data integrity during transfer of the data or information. Beneficially, a need for repetitive identity re-
35 verification at each port is reduced or eliminated and a single source of truth across jurisdictions is established.

Linkage to Digital Transactions and Machine-Readable Code Authentication

[0047] Each version-controlled vessel identity record or vessel information record may be linked to digital identity used for port operations and authentication events, such as real-time machine-readable code authentication for document signing, time-permissioned machine-readable code with 6-digit PIN for port access, cryptographically generated digital ship stamps, etc. Some non-limiting examples of the machine-readable code can be a Quick Response (QR) code and a barcode.

[0048] The identity-linked machine-readable code can be embedded with a current identity version or vessel information record (e.g., V2). Advantageously, this allows all digital transactions to be traceable to a verified and most recent vessel profile.

Issuance of Time-Permissioned Machine-Readable Code Post-Identity Verification

[0049] Once the vessel's identity has been successfully verified during the Pre-Arrival Notification (PAN) process, a time-permissioned machine-readable code such as a QR code may be generated by the Digital Identity Service Provider System. The machine-readable code may be embedded with the validated vessel identity, a scheduled port stay window, access permission(s), etc. The machine-readable code, together with a second authentication factor, may be issued by a Port Authority or a relevant government agency, and delivered to the vessel's designated operator or agent through secured communication channels. A non-limiting example of the second authentication factor can be a personal identification number (PIN). The PIN may be a 6-digit PIN. Beneficially, only authenticated and authorized vessels receive valid entry credentials, hence secure and regulated port access is ensured.

Session Termination

[0050] Figure 5 is a schematic representation 500 illustrating a session termination process, according to an example embodiment. The authentication method for maritime operations may allow session termination in the event of suspected compromise, operational changes, cancellation of planned activities, etc. Session termination may include revocation of issued authentication tokens, machine-readable codes such as QR codes, or signing sessions. The revocation may be immediate. Revocation can also be based on predefined conditions. Some examples of the predefined conditions may be device mismatch, AIS location anomaly and multiple failed authentication attempts. As shown in Figure 5, session termination may include

expiration of the issued authentication tokens and/or machine-readable codes such as QR codes.

- 5 [0051] As an example, in the event that the vessel's planned route changes, such as skipping a port call or altering its sequence of stops, the authentication method may revoke pending signing or verification requests that are no longer relevant. As shown in Figure 5, once revoked, an associated credential or session may be marked as invalid across all connected systems, and any subsequent signing or verification actions using the revoke signing or verification requests can be processed with a "revoked" status
- 10 flag. This ensures that while signing of documents may still technically occur, all involved parties can be notified in a short period of time or immediately that the credential was revoked at the time of use. The signed document and its metadata may display a visible warning or "revoked" indicator, and the revocation event may be propagated to all linked parties and systems in real time. All revocation actions can be
- 15 logged in an audit trail with timestamps, initiator identity, affected transaction references, and a reason for revocation in order to maintain transparency and compliance.

Crew Identification and Assignment of Digital Identity

- 20 [0052] The Digital Identity Service Provider System or the Identity Authentication system can include an Identified Crew feature. The Identified Crew feature may facilitate verification of identities of crew members involved in digital shipboard activities. Advantageously, operational transparency and accountability can be enhanced.
- 25

- [0053] Ship operators or the master of the vessel can input crew member details such as name, role, email address, and duration of service onboard into the Digital Identity Service Provider System or the Identity Authentication system via the Digital Identity
- 30 Service Provider Application. Upon entry, the Digital Identity Service Provider System or the Identity Authentication system may generate a unique, time-permissioned machine-readable code such as a QR code that represents the individual's identity and role on the vessel. This machine-readable code may be sent via email and may be valid for a specified period of time.

35

[0054] When the machine-readable code is scanned during an action (e.g., document signing or submission), the authentication method may verify the vessel's identity and an identity of a crew member performing the action, if available. The dual-layer verification advantageously enhances traceability and accountability for each digital transaction made on behalf of the vessel, and ensures that actions can be clearly attributed to specific, identified individuals.

Secure Crew Access

[0055] In addition, the vessel may pre-register the crew members using the Digital Identity Service Provider Application and assign the crew members digital identities with validity periods. The validity periods may be configurable.

[0056] After the pre-registration, each registered crew member may receive a secure login credential to access the Digital Identity Service Provider Application and/or access to an in-app Authenticator (e.g., QR code scanner) for real-time identity verification during port operations. Beneficially, this ensures that only authorized and verified individuals can perform vessel-related digital actions such as form submissions, QR-based authentications or document signing, which significantly reduces a risk of unauthorized access or fraudulent activity.

Authentication Code Generation

[0057] Figure 6 is a flowchart 600 illustrating an authentication code generation, according to an example embodiment. As shown in Figure 6, the authentication code may be generated based on pre-defined inputs. Some examples of the pre-defined inputs may be a vessel identity, a Digital Identity Service Provider System user account number, a date and/or time and a random salt.

Vessel Identity Source

[0058] The authentication method may allow multiple vessel identity sources to be used for the generation of the authentication code. The vessel identity sources can facilitate extraction of vessel identity such as an International Maritime Organization (IMO) number, a Digital Identity Service Provider System number and a Local Registration Vessel number. The Local Registration Vessel number may be dependent on a vessel's identification system in the region of operation. Examples of the Local

Registration Vessel number can be an EIN (European Number of Identification), a SRS (Singapore Registry of Ships) number and other local vessel identification number.

Random Salt

- 5
- [0059] According to one embodiment, the random salt may be stored on a server of the Identity Authentication system and on one or more authorized devices. The random salt used in the authentication code generation may be securely stored both on a central server of the Digital Identity Service Provider System or the Identity
- 10 Authentication system and locally on one or more authorized client devices. By storing the random salt locally on the authorized client devices, the authorized client devices which may be offline-capable can generate valid authentication codes independently, even when disconnected from the internet.
- 15 [0060] In some implementations, the random salt may be refreshed periodically. Further, the refreshed random salt may be transmitted to the one or more authorized devices for offline generation of the authentication code. The random salt may be refreshed on a periodic basis (e.g., on a monthly basis). The refreshed random salt may be transmitted to the authorized client devices through secured over-the-air
- 20 synchronization mechanisms. Beneficially, resilience against replay or prediction attacks is ensured.

Algorithm for Code Generation

- 25 [0061] The authentication code generation method may combine the pre-defined inputs such as a selected vessel identity (e.g., IMO, Digital Identity Service Provider System number or Local Vessel Registration number), the Digital Identity Service Provider Account Number of the user, the real-time date and time, and the random salt. The pre-defined inputs may be passed through a pre-defined algorithm to generate the
- 30 authentication code.

QR Code Generation

- [0062] As mentioned above, at step 104 of the authentication method for maritime
- 35 operations, the machine-readable code is generated using the Identity Authentication system upon validation of the PAN vessel identity information. According to one embodiment, the machine-readable code may be a real-time QR code or a time-

permitted QR code. The real-time QR code and the time-permitted QR code may be used for identity verification and secure digital interactions in the maritime operations.

5 *Real-time QR Code*

[0063] The authentication code may be embedded within the real-time QR code, which may contain metadata such as the vessel's IMO number, crew name, crew role (e.g., Master, Cargo Officer), and a secure URL that can link to the authentication log for additional verification. The QR code may be time-bound (e.g., for 30 seconds) and may be dynamically regenerated based on a session state and a permission logic. Beneficially, the QR code remains valid only for a limited authentication window to prevent reuse or interception. In the event that the QR code is scanned using an authorized application integrated with the Digital Identity Service Provider System or the Identity Authentication system, the authentication code may be validated in real time. Further, when internet access becomes available, more details can be retrieved from the central server of the Digital Identity Service Provider System or the Identity Authentication system to complete a verification process.

20 [0064] Figure 7 is a schematic representation 700 illustrating information embedded in a real-time QR code, according to an example embodiment. As shown in Figure 7, the real-time QR code may comprise the vessel identity, a Digital Identity Service Provider System account number, an account name, an account role, the authentication code, a geographic location (when available) and detailed information.

25 [0065] The vessel identity may be a unique identifier for the vessel. The vessel identity can allow the vessel to be correctly identified. The Digital Identity Service Provider System account number may be a specific account number associated with the crew member within the Digital Identity Service Provider System. The account name may be a name of the individual crew associated with the account, for example the crew member or an officer. The account role may be a role of an individual, such as Master, cargo officer, chief engineer of a vessel, which can provide context for signing authority on behalf of an operator of the vessel.

35 [0066] The authentication code may be a time-sensitive code generated by combining the IMO number, the Digital Identity Service Provider System account number, and the real-time date and/or time. The authentication code may be valid for a pre-determined

period of time such as 30 seconds, after which it may automatically expire and refresh. The geographic location may be the vessel's real-time location data such as latitude and longitude at a time of generation of the real-time QR code. The geographic location may be included if location data is available at a time of authentication (i.e., during online usage). The detailed information can be a URL. The URL may contain embedded information such as the IMO number, the Digital Identity Service Provider System account number, and the authentication code. The URL can be used to retrieve more details and verify authenticity of a signing event.

- 10 [0067] A non-limiting example of information encoded in the real-time QR code can be as follows:

```

    {
      "authenticatorCode":989382,
      "codeType":"imoNumber",
      "imoNumber":"9767912",
      "singaporeLicenseNumber":"sb2334",
      "shipDigital Identity Service Provider Number":"70222569821",
      "vesselName": "PCGVESSEL"
      "accountNo":"87039492",
      "accountName":"Chris",
      "accountRole": "Cargo Officer",
      "getInfo":"http://localhost:8480/authentication/doc/getInfo?codeTypeValue=976
      7912&authenticatorCode=989382&accountNo=87039492"
    }
  
```

25

Time-permissioned QR Code

- [0068] In addition to real-time authentication, the time-permissioned QR codes may be issued for scheduled port-based operations. When the vessel submits a Pre-Arrival Notification (PAN) before entering port waters, validation of the identity of the vessel may be performed using data retrieved from the Ship Information Database. Upon successful validation, the time-permissioned QR code may be generated. The time-permissioned QR code may be programmed to remain valid only during a vessel's authorized port stay window. In some implementations, the authentication code embedded in the time-permissioned QR code may be valid for the port stay window of the vessel.

[0069] The authentication method for maritime operations may further comprise generating a personal identification number (PIN) using the Identity Authentication system after generating the time-permissioned QR code. The vessel may be
5 authenticated based on the generated machine-readable code, the PIN and the Ship Information Database. The PIN may be a six-digit PIN. Beneficially, the PIN can serve as a second factor of authentication. Both the time-permissioned QR code and the PIN may be transmitted to the vessel's operator or designated agent via a welcome email issued by the Port Authority.

10 [0070] The time-permissioned QR code can serve as a temporary digital access credential and can be used in specific port activities, including but not limited to port entry and clearance procedures, bunkering operations, customs inspection processes and crew onboarding or disembarkation authentication.

15 [0071] Advantageously, the real-time QR code and the time-permissioned QR code enable secure and permission-controlled execution of maritime procedures, replacing a need for paper-based passes or manual verifications.

20 Document Signing Workflow

[0072] The authentication method may facilitate a secure, flexible document signing process designed for maritime environment where connectivity may vary. Figure 8 is a flowchart 800 illustrating an electronic document signing process, according to an
25 example embodiment. As shown in Figure 8, the authentication method may enable document authentication and digital signing through two modes of operation - online document signing and offline document signing. Advantageously, both modes of operation ensure integrity, authenticity, and traceability of a signing event, regardless of connectivity status.

30 *Online Document Signing*

[0073] In an online environment, the document signing process may leverage active connectivity to validate identities in real time. The online document signing process
35 may comprise a counterparty, such as a bunker supplier, a surveyor, or a government officer, scanning either the real-time QR code or the time-permissioned QR code using

the authorized application integrated with the Digital Identity Service Provider System or Identity Authentication system.

5 **[0074]** Upon scanning either the real-time QR code or the time-permissioned QR code, the verified vessel identity from the Ship Information Database and the vessel's real time geographic location may be retrieved. A digital stamp, which may be cryptographically generated and uniquely tied to a timestamp, the vessel identity, and a document creator may also be retrieved.

10 **[0075]** A real-time geographic location comparison may be performed. When applicable, the real-time geographic locations of both participating parties (e.g., a bunker barge and a receiving vessel or oil terminal) may be compared and/or restricted to a defined location as specified by a user. If the vessels are not within a defined proximity threshold, an alert or warning may be issued to signing parties and to an
15 audit trail to indicate a potential anomaly. However, the signing process may still proceed with this alert in place. Beneficially, this allows for operational flexibility while maintaining traceability and oversight. The method also enhances situational awareness and helps detect potentially fraudulent or misaligned signing activities without fully blocking valid exceptions.

20 **[0076]** According to one embodiment, the authentication method for maritime operations may further comprise generating a digital stamp using the Identity Authentication system and applying the digital stamp to an electronic document using the Identity Authentication system. The electronic document can be an electronic
25 bunkering delivery note (eBDN). Application of the digital stamp may comprise visibly embedding the digital stamp as part of a signed output.

30 **[0077]** In some implementations, the digital stamp may comprise a digital stamp QR code and the digital stamp QR code may embed a transaction identifier. Each digital stamp may be uniquely generated for the particular electronic document and may include a timestamp of the signing, the document creator, the verified vessel identity details (e.g., IMO number, vessel name), a signer (e.g., crew) details and an embedded machine-readable code such as the digital stamp QR code that can link back to an authentication event and a transaction metadata or the transaction identifier
35 for audit purposes.

[0078] Figure 9 is an image 900 of the digital stamp, according to an example embodiment. As shown in Figure 9, the digital stamp QR code can be positioned in the middle of the digital stamp.

- 5 [0079] After successful verification, the electronic document such as the eBDN may be signed digitally using a signing interface. The signing event may be recorded in the Digital Identity Service Provider System or Identity Authentication system, and a unique transaction ID may be generated. An audit log capturing all relevant verification and signing metadata may be securely stored and made available for later review by
- 10 authorized parties. Beneficially, the online document signing process allows document authenticity to be confirmed in real time, including contextual data such as a vessel's physical location and a signing party's verified credentials.

Offline Document Signing

- 15 [0080] In scenarios which network connectivity may be unavailable or unstable, such as during offshore operations or within restricted port zones, secure offline document signing may be performed through a local verification process between two devices. One of the devices may be operated by the vessel and by using the Digital Identity
- 20 Service Provider Application. The other device may be operated by the counterparty such as a bunker supplier or a surveyor.

- [0081] Figure 10 is a flowchart 1000 illustrating an offline electronic document signing process, according to an example embodiment. As shown in Figure 10, the offline
- 25 electronic document signing process may include a step to initiate scanning of the machine-readable code such as the QR code. The counterparty may use a third-party authorized application on his device to scan the real-time QR Code displayed on the Digital Identity Service Provider Application running on the vessel's device.

- 30 [0082] Local verification may then be performed via the Digital Identity Service Provider Application. Specifically, after scanning the real-time QR Code, the counterparty's device can obtain the embedded authentication code and send it locally (i.e., offline) to the Digital Identity Service Provider Application, which may also be running on the counterparty's device, for verification.

- 35 [0083] The Digital Identity Service Provider Application may verify the authentication code using cached identity data and the locally stored random salt which may have been updated from the Digital Identity Service Provider server. Upon successful

verification, the Digital Identity Service Provider Application may return verification results and the digital stamp which may be uniquely tied to the vessel identity, the timestamp, the authentication code, and a document context. The digital stamp may be a base 64 digital stamp.

5

[0084] The third-party application may receive verified digital stamp data from the Digital Identity Service Provider Application, decode the verified digital stamp data to a picture format and apply the picture format digital stamp to the electronic document such as the eBDN.

10

[0085] The digital stamp can act as a cryptographic attestation of the vessel's verified identity. Further, the digital stamp may embed the QR code that can be scanned at a later time to retrieve a link to a transaction log once the device reconnects to a network (i.e. becomes online).

15

[0086] Once the device regains internet connectivity, the locally stored data can be synchronized with the Digital Identity Service Provider System or the Identity Authentication system. The Digital Identity Service Provider System or the Identity Authentication system may send a query to the server to retrieve full vessel identity information (e.g., IMO number, vessel name, operator ID) and push a verification log to the Digital Identity Provider System cloud server so that a complete and up-to-date transaction history can be stored.

20

[0087] The offline verification log may contain a plurality of data points. The data points may include a vessel identity number of the vessel, signer (i.e. crew) details such as his/her name and role, a type of the machine-readable code used such as the real-time QR code or the time-permissioned QR code, the digital stamp issued (e.g., the base 64 format digital stamp), the real time geographic location, a device ID and third-party application ID used for scanning the machine-readable code, the timestamp of the signing event and the verification result (e.g., pass/fail or matched/unmatched).

25

30

[0088] Advantageously, the offline electronic document signing process ensures secure and traceable document signing even in connectivity-constrained environments, with an ability to verify transactions retroactively once device(s) reconnect to the network. The embedded machine-readable code such as the QR code in the digital stamp can allow any party to scan the signed document at a later time and retrieve a full transaction audit trail from the server.

35

Retrieval of Data Using the Embedded Machine-readable Code in The Digital Stamp

- [0089] Each digital stamp applied to the signed document includes the embedded machine-readable code such as the QR code. The embedded machine-readable code may serve as a reference pointer to corresponding authentication and transaction events. When scanned using the authorized application or a web-based verifier, the embedded machine-readable code can allow retrieval of a plurality of verifiable metadata. Some examples of the plurality of verifiable metadata may be the IMO number and the local registration vessel number, a vessel identity profile, the Digital Identity Service Provider account number, the crew identity, the type of machine-readable code used, the timestamp of the signing event, the geographic location (if available), a Digital Stamp hash, a device and application ID, the verification status and the transaction ID.
- [0090] The IMO number and the local registration vessel number may be a unique identifier for the vessel involved. The vessel identity profile may include a vessel name, a flag state, the operator and other identifiers of the vessel. The Digital Identity Service Provider account number may be the verified identity of the vessel. The crew identity may be the verified identity of the signing crew member or officer. The type of machine-readable code used may indicate whether the document was signed using the real-time QR code or the time-permissioned QR code. The timestamp of the signing event may indicate an exact date and time when the document was signed. The geographic location may be AIS-derived or device-based coordinates at the time of signing the document. The Digital Stamp hash may be a cryptographic hash of the digital stamp applied to the document for authenticity verification. The device and application ID may be the ID of the authorized third-party application and device used during the signing event. The verification status may be an indication of whether the authentication was successful (e.g., matched, proximity check passed). The transaction ID may be a unique identifier for the signing and authentication event, allowing traceability in audit systems.

Geo Location Tag for Digital Signing

- [0091] The digital signing process may include geo-location tagging to enhance operational security and regulatory compliance. Each signing or verification event may

be bound to vessel location data, such as AIS-reported coordinates, port calls, or predefined geographic zones.

5 [0092] For example, digital signatures may only be executed when the vessel is within an authorized region, port, or territorial jurisdiction. Location tags may be combined with date-bound and time-bound restrictions to further control a validity of signatures. Any attempt to perform authentication or execute documents from outside the permitted geographic parameters (e.g., an unregistered vessel location, an unauthorized device attempting to spoof position, or a disallowed location or port) can
10 automatically generate a warning flag on both the document and a corresponding transaction record.

[0093] For example, a vessel operator may configure policies such that digital signing is only permitted when the vessel's AIS location confirms that the vessel has departed
15 Port A, is currently within Port B, and is scheduled to arrive at Port C. Beneficially, this geo-location binding ensures that sensitive transactions are executed exclusively within approved operational zones, thereby reducing the risk of fraudulent or unauthorized actions from outside the intended jurisdiction.

20

Digital Audit Trail and Verification Record

[0094] Every instance of digital identity usage and document signing using the Digital Identity Service Provider System or the Identity Authentication system may generate a
25 secure and verifiable audit trail. Beneficially, accountability, transparency and traceability for maritime transactions involving digital authentication are enhanced. The audit trail can be automatically created upon each signing event and may include a plurality of data points. Non-limiting examples of the plurality of data points can be the authentication code used during verification, the relevant vessel and crew digital
30 identifiers which may include the IMO number and the account number of the signer, the type of machine-readable code scanned (e.g., the real-time QR code or the time-permissioned QR code, the real-time geographic location of the vessel at the time of signing the document (if available), the timestamp of the signing event and the corresponding digital signature, the application ID of a third-party tool or device used to
35 scan and process the machine-readable code, and the unique transaction ID generated for reference and traceability.

- [0095] All records may be securely stored in a distributed logging infrastructure of the Digital Identity Service Provider System or the Identity Authentication system. Logs can be accessible by authorized entities such as port authorities, ship operators, classification societies, and maritime regulatory bodies. The audit trail can be queried or exported to assist with compliance audits, investigations, and historical reviews.

Country-Specific Deployment

- [0096] Decentralized deployment of the Ship Information Database system may be performed to accommodate legal and regulatory requirements of different jurisdictions. Each participating country or port authority may implement its own independent instance of Ship Information Database. Advantageously, localized control and policy enforcement is facilitated.

- [0097] Specifically, each national or regional implementation may host and manage its own vessel identity registry, including the IMO and local identifiers. The national or regional implementation may also maintain a dedicated hash repository for digital identities and QR-related cryptographic data. Further, the national or regional implementation may define jurisdiction-specific policies, such as validity windows for time-permissioned QR codes tied to port calls, expiry timeframes for PIN-based access credentials and data retention policies for audit logs and transaction records.

- [0098] Beneficially, the flexible deployment model ensures that while vessel and crew identities can be universally interoperable, each jurisdiction retains sovereign control over its own digital identity infrastructure. Interoperability can be maintained through standardized machine-readable code structures such as QR structures, encryption protocols, and hash verification algorithms, hence enabling seamless international operations.

eDocument Generation and Signing Workflow Based on BMT Data

- [0099] Figure 11 is a flowchart 1100 illustrating a document signing process for electronic bunker delivery notes (eBDNs), according to an example embodiment. Figure 12 is a flowchart 1200 illustrating a document signing process for eBDNs, according to another example embodiment.

- [00100] As shown in Figure 11 and Figure 12, the document signing process for the eBDNs can be an automated process. The eBDNs may be automatically generated and signed by integrating real-time operational data, for example Bunker Mass Transfer (BMT) values. Advantageously, the automated document signing process for eBDNs enhances efficiency and accuracy in maritime fueling operations by reducing manual data entry and expediting the verification process.

Data Retrieval from BMT Measurement System

- 10 [00101] Upon completion of a bunker transfer operation, a final BMT value representing a measured mass of fuel delivered may be retrieved through an Application Programming Interface (API) from a BMT measurement system. The BMT value may serve as an operational data point for the document generation.

15 *Auto-generation of eBDN*

- [00102] Once the BMT value is received, it may be automatically populated into a corresponding eBDN template within a Digital Bunkering System. Other relevant operational and identity metadata (e.g., vessel name, IMO number, supplier, date/time) may also be pre-filled using data from the Digital Identity Service Provider System or the Identity Authentication system and the Ship Information Database.

Dual Acknowledgment Workflow

- 25 [00103] Both a supplying party (e.g., a bunker barge operator) and a receiving party (e.g., a chief engineer or a cargo officer) may be required to review and acknowledge the pre-filled data on an eBDN system interface. The eBDN system interface may be a webpage or a display on a remote device application such as a mobile application or an application installed on a tablet. Beneficially, a dual-party confirmation ensures operational agreement and data accuracy prior to signing of the eBDN.

Digital Signing and Digital Stamp Application

- 35 [00104] After both the supplying party and the receiving party acknowledge the pre-filled data on the eBDN system interface, a digital signing phase may be triggered. Each of the supplying party and the receiving party may use the real-time QR code or

the time-permissioned QR code for identity verification. A digital stamp containing data such as the timestamp, the vessel identity and/or the real-time geographic position (when available) may be applied to a signed document as an embedded element. Beneficially, the digital stamp ensures that a signature is securely bound to the vessel's

5 digital identity and operational context at the time of signing the document.

[00105] Figure 13 is an example image 1300 of the eBDN of Figure 11 and/or 12. As shown in Figure 13, the digital stamps of both the supplying party and the receiving party may be applied to the eBDN.

10

Other Use Cases And Applications

Other Applications

15 [00106] The document signing process for eBDNs may not be limited to eBDNs. The document signing process may be applicable to other maritime document workflows. Some non-limiting examples of the other maritime document workflows can be electronic Pre-Arrival Notifications (ePANS) submissions to port authorities, general declaration documentation such as vessel declarations and cargo-related submissions,

20 port clearance and departure submissions to port authorities for departure declaration, cargo manifests for goods transport and regulatory compliance and crew-related submissions such as crew lists, shore leave passes, and identity verification records.

[00107] The document signing process may support interactions between

25 multiple stakeholders including, but not limited to, the port authorities, customs authorities, terminal operators, vessel agents, the crew members, service providers, and the suppliers. Beneficially, a unified and secure transaction environment is facilitated.

Other Use Cases

30

[00108] Port clearance may be a regulatory process involving multiple parties, such as the vessel master, the appointed shipping agent, the port clearance platform, and the port clearance authority.

35

[00109] The authentication method for maritime operations may allow the vessel masters and the agents to authenticate into different platforms using the single, verifiable digital identity tied to the Ship Information Database. The authentication

method may ensure that all PAN (Pre-Arrival Notification), GD (Goods Declaration), and port clearance certificate submissions are completed and exchanged under authenticated vessel and agent identities. Advantageously, the authentication method eliminates fragmented processes that rely on repeated manual submissions, multiple
5 logins, and redundant communications between the ship operators and the agents. Errors in vessel particulars, delays in document forwarding, or unauthorized access to documents which can lead to compliance risks and operational inefficiencies are also reduced or eliminated.

10 **[00110]** Some features used in the port clearance may be verified vessel data source, unified authentication across platforms, automated distribution and audit trail, controlled access to the documents and integration without duplication.

[00111] With respect to the feature of verified vessel data source, vessel
15 particulars may be pre-filled using data from the Ship Information Database and geographic location-linked records so that clearance submissions can be based on most accurate and up-to-date information.

[00112] With respect to the feature of unified authentication across platforms,
20 both the vessel master and the agent may authenticate using the Digital Identity Service Provider Application, which may use the real-time QR codes, time-based permissions and/or PIN validation to ensure only authorized individuals can access or submit clearance documents.

25 **[00113]** With respect to the feature of automated distribution and audit trail, once a submission or approval is completed, summary data and signed documents may be automatically distributed to all relevant parties (e.g., the vessel master, the agent, the port authority) and recorded in an immutable audit trail. This advantageously eliminates a need for manual forwarding and provides traceability for compliance.

30 **[00114]** With respect to the feature of controlled access to the documents, the ship operators can restrict or grant access of clearance documents to specific parties (e.g., head office, charterers) through the Digital Identity Service Provider Application. Beneficially, confidentiality is ensured.

35 **[00115]** With respect to the feature of integration without duplication, clearance systems such as the Port Authority Platform may only receive required operational data, while commercial or private details remain secured within the Digital Identity

Service Provider Application. Advantageously, duplication and overexposure of information is reduced or eliminated.

[00116] The present specification also relates to an authentication system for maritime operations. The authentication system comprises an Identity Authentication system configured to validate Pre-Arrival Notification (PAN) vessel identity information based on a latest version of a vessel information record stored in a Ship Information Database. The vessel information record comprises validated vessel identity information. The vessel identity information is validated based on government and/or regulatory boards databases. The Identity Authentication system is further configured to generate a machine-readable code upon validation of the PAN vessel identity information. The machine-readable code embeds the latest version of the vessel information record and an authentication code. The embedded latest version of the vessel information record and authentication code are valid for a pre-determined period of time. The authentication code comprises a random salt. The Identity Authentication system is also configured to authenticate a vessel based on the generated machine-readable code and the Ship Information Database.

[00117] In some implementations, the Identity Authentication system may be further configured to obtain an authorization message from an authorized device associated with the vessel to transmit the latest version of the vessel information record to a selected port system. The Identity Authentication system may be further configured to apply version control to the vessel information record stored in the Ship Information Database.

[00118] The random salt may be stored on a server of the Identity Authentication system and on one or more authorized devices. The random salt may be refreshed periodically and the refreshed random salt may be transmitted to the one or more authorized devices for offline generation of the authentication code.

[00119] According to one embodiment, the machine-readable code can be a real-time QR code or a time-permissioned QR code. The authentication code embedded in the time-permissioned QR code may be valid for a port stay window of the vessel. The Identity Authentication system may be further configured to generate, on a condition that the machine-readable code is a time-permissioned QR code, a personal identification number (PIN). The vessel may be authenticated based on the generated machine-readable code, the PIN and the Ship Information Database.

[00120] The Identity Authentication system may be further configured to generate a digital stamp and apply the digital stamp to an electronic document. The digital stamp may comprises a digital stamp QR code and the digital stamp QR code
5 may embed a transaction identifier.

[00121] Figure 14 is a schematic diagram of a computer system suitable for use in executing at least some steps of the authentication method for maritime operations.

10 [00122] The following description of the computer system / computing device 1400 is provided by way of example only and is not intended to be limiting.

[00123] As shown in Figure 14, the example computing device 1400 includes a processor 1404 for executing software routines. Although a single processor is shown
15 for the sake of clarity, the computing device 1400 may also include a multi-processor system. The processor 1404 is connected to a communication infrastructure 1406 for communication with other components of the computing device 1400. The communication infrastructure 1406 may include, for example, a communications bus, cross-bar, or network.

20 [00124] The computing device 1400 further includes a main memory 1408, such as a random access memory (RAM), and a secondary memory 1410. The secondary memory 1410 may include, for example, a hard disk drive 1412 and/or a removable storage drive 1414, which may include a magnetic tape drive, an optical disk drive, or
25 the like. The removable storage drive 1414 reads from and/or writes to a removable storage unit 1418 in a well-known manner. The removable storage unit 1418 may include a magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 1414. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 1418 includes a computer readable storage medium
30 having stored therein computer executable program code instructions and/or data.

[00125] In an alternative embodiment, the secondary memory 1410 may additionally or alternatively include other similar devices for allowing computer programs or other instructions to be loaded into the computing device 1400. Such
35 devices can include, for example, a removable storage unit 1422 and an interface 1420. Examples of a removable storage unit 1422 and interface 1420 include a removable memory chip (such as an EPROM or PROM) and associated socket, and

other removable storage units 1422 and interfaces 1420 which allow software and data to be transferred from the removable storage unit 1422 to the computer system 1400.

[00126] The computing device 1400 also includes at least one communication interface 1424. The communication interface 1424 allows software and data to be transferred between computing device 1400 and external devices via a communication path 1426. In various embodiments, the communication interface 1424 permits data to be transferred between the computing device 1400 and a data communication network, such as a public data or private data communication network. The communication interface 1424 may be used to exchange data between different computing devices 1400 which such computing devices 1400 form part of an interconnected computer network. Examples of a communication interface 1424 can include a modem, a network interface (such as an Ethernet card), a communication port, an antenna with associated circuitry and the like. The communication interface 1424 may be wired or may be wireless. Software and data transferred via the communication interface 1424 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 1424. These signals are provided to the communication interface via the communication path 1426.

[00127] Optionally, the computing device 1400 further includes a display interface 1402 which performs operations for rendering images to an associated display 1430 and an audio interface 1432 for performing operations for playing audio content via associated speaker(s) 1434.

[00128] As used herein, the term "computer program product" may refer, in part, to removable storage unit 1418, removable storage unit 1422, a hard disk installed in hard disk drive 1412, or a carrier wave carrying software over communication path 1426 (wireless link or cable) to communication interface 1424. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 1400 for execution and/or processing. Examples of such storage media include floppy disks, magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, USB memory, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 1400. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs,

instructions and/or data to the computing device 1400 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

5

[00129] The computer programs (also called computer program code) are stored in main memory 1408 and/or secondary memory 1410. Computer programs can also be received via the communication interface 1424. Such computer programs, when executed, enable the computing device 1400 to perform one or more features of
10 embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 1404 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 1400.

15 **[00130]** Software may be stored in a computer program product and loaded into the computing device 1400 using the removable storage drive 1414, the hard disk drive 1412, or the interface 1420. Alternatively, the computer program product may be downloaded to the computer system 1400 over the communications path 1426. The software, when executed by the processor 1404, causes the computing device 1400 to
20 perform functions of embodiments described herein.

[00131] It is to be understood that the embodiment of Figure 14 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 1400 may be omitted. Also, in some embodiments, one or more
25 features of the computing device 1400 may be combined together. Additionally, in some embodiments, one or more features of the computing device 1400 may be split into one or more component parts.

[00132] It will be appreciated by a person skilled in the art that numerous
30 variations and/or modifications may be made to the embodiments. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. An authentication method for maritime operations, comprising:
validating, using an Identity Authentication system, Pre-Arrival Notification
5 (PAN) vessel identity information based on a latest version of a vessel information
record stored in a Ship Information Database, wherein:
the vessel information record comprises validated vessel identity
information; and
the vessel identity information is validated based on government and/or
10 regulatory boards databases;
generating, upon validation of the PAN vessel identity information and using the
Identity Authentication system, a machine-readable code, wherein:
the machine-readable code embeds the latest version of the vessel
information record and an authentication code;
15 the embedded latest version of the vessel information record and
authentication code are valid for a pre-determined period of time; and
the authentication code comprises a random salt; and
authenticating, using the Identity Authentication system, a vessel based on the
generated machine-readable code and the Ship Information Database.
20
2. The method of claim 1, further comprising:
before validating the PAN vessel identity information based on the latest version
of the vessel information record stored in the Ship Information Database, obtaining,
using the Identity Authentication system, an authorization message from an authorized
25 device associated with the vessel to transmit the latest version of the vessel
information record to a selected port system.
3. The method of claim 1, further comprising:
applying, using the Identity Authentication system, version control to the vessel
30 information record stored in the Ship Information Database.
4. The method of claim 2, wherein the random salt is stored on a server of the
Identity Authentication system and on one or more authorized devices.
- 35 5. The method of claim 4, wherein:
the random salt is refreshed periodically; and

the refreshed random salt is transmitted to the one or more authorized devices for offline generation of the authentication code.

6. The method of claim 1, wherein the machine-readable code is a real-time QR code or a time-permissioned QR code.

7. The method of claim 6, wherein the authentication code embedded in the time-permissioned QR code is valid for a port stay window of the vessel.

8. The method of claim 6, further comprising:
after generating the time-permissioned QR code, generating, using the Identity Authentication system, a personal identification number (PIN), wherein the vessel is authenticated based on the generated machine-readable code, the PIN and the Ship Information Database.

9. The method of claim 1, further comprising:
generating, using the Identity Authentication system, a digital stamp; and
applying, using the Identity Authentication system, the digital stamp to an electronic document.

10. The method of claim 9, wherein:
the digital stamp comprises a digital stamp QR code; and
the digital stamp QR code embeds a transaction identifier.

11. An authentication system for maritime operations, comprising:
an Identity Authentication system configured to:
validate Pre-Arrival Notification (PAN) vessel identity information based on a latest version of a vessel information record stored in a Ship Information Database, wherein:

the vessel information record comprises validated vessel identity information; and

the vessel identity information is validated based on government and/or regulatory boards databases;

generate, upon validation of the PAN vessel identity information, a machine-readable code, wherein:

the machine-readable code embeds the latest version of the vessel information record and an authentication code;

the embedded latest version of the vessel information record and authentication code are valid for a pre-determined period of time; and

5 the authentication code comprises a random salt; and

authenticate a vessel based on the generated machine-readable code and the Ship Information Database.

12. The system of claim 11, wherein the Identity Authentication system is further
10 configured to obtain an authorization message from an authorized device associated with the vessel to transmit the latest version of the vessel information record to a selected port system.

13. The system of claim 11, wherein the Identity Authentication system is further
15 configured to apply version control to the vessel information record stored in the Ship Information Database.

14. The system of claim 12, wherein the random salt is stored on a server of the Identity Authentication system and on one or more authorized devices.

20

15. The system of claim 14, wherein:
the random salt is refreshed periodically; and
the refreshed random salt is transmitted to the one or more authorized devices
for offline generation of the authentication code.

25

16. The system of claim 11, wherein the machine-readable code is a real-time QR code or a time-permissioned QR code.

17. The system of claim 16, wherein the authentication code embedded in the time-
30 permissioned QR code is valid for a port stay window of the vessel.

18. The system of claim 16, wherein the Identity Authentication system is further
configured to generate, on a condition that the machine-readable code is a time-
permissioned QR code, a personal identification number (PIN), wherein the vessel is
35 authenticated based on the generated machine-readable code, the PIN and the Ship Information Database.

19. The system of claim 11, wherein the Identity Authentication system is further configured to:

- 5 generate a digital stamp; and
 apply the digital stamp to an electronic document.

20. The system of claim 19, wherein:

- the digital stamp comprises a digital stamp QR code; and
 the digital stamp QR code embeds a transaction identifier.
10