An outline of an international public key infrastructure for the maritime sector

ISTS Report R5.3
V1 – 2024-11-22

MARITIME ITS

Intelligent Ship Transport System

Document information

Title	R5.3 An outline of an international public key infrastructure for the maritime sector
Classification	Public

Editors and main contributors	Company
Ørnulf Jan Rødseth (ØJR)	ITS Norway

Rev.	Who	Date	Comment
0.1	ØJR	2024-11-04	First draft
0.2	ØJR	2024-11-05	Corrected references
0.3	ØJR	2024-11-05	Added access authentication, caching and identity requirements
1.0	ØJR	2024-11-22	Final edit for release

Table of Contents

Executive Summary

Digital signatures will be important for safe and secure digitalization in the maritime sector (section 3). Access to such signatures is normally managed in what is called a public key infrastructure (PKI) and several such PKIs are already in use by land-based parties. However, shipping is an international business, and this creates some special requirements to a PKI for use in international shipping (section 4). Therefore, a dedicated maritime PKI is proposed in section 5 and some general guidance for how the private key should be managed onboard are provided in section 6.

Definitions

CA (Certificate authority): Entity trusted to create, assign and revoke public key certificates.

There are several variants of this definition, but the key point here is "*trusted*". In the international maritime world, this could be IMO itself and/or a flag states. There may be one or more CA. The CA may also delegate the issuance of certificates to a sub-CA. In this case, the sub-CA can also be named a CA. Note that "authority" does not imply any government authorization but only denotes that the party is trusted.

Digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to verify the source and integrity of the data unit [5].

The term *electronic signature* is sometimes used for a data block with a similar function. In this document, the term *digital signature* will be used.

Certificate (Public key certificate): Public key information of an entity signed by the CA and thereby rendered unforgeable [5].

In this document, the term *certificate* will be used for the public key certificate unless otherwise qualified, e.g. as in ship or crew certificate.

Hash (function/code): In the context of cryptography, a hash function is a one-way function that calculates a fixed length hash number from a data set. It is generally not possible to change the data set without also changing the hash code, thus the one-way property.

Key: A key is a data structure that is used to sign or encrypt a message (the private key) or to decrypt or validate the same (the public key).

PKI (public key infrastructure): Infrastructure used in the relation between a private key holder and a relying party that allows the relying party to use a certificate relating to the key holder, using a public key dependent security service and that includes a certification authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy, and methods to validate the certification practice [5].

Root certificate: Certificate created by the CA and used as the trust anchor in a PKI.

The root certificate is normally signed by the CA itself and trust in the root certificate and the CA must be created based on how the root certificate is distributed, e.g. through a distribution mechanism that is trusted in itself.

A sub-CA will sign its root certificate with that of the CA's root certificate. However, for the purpose of this document, both will be termed just root certificate.

Sub-CA (Subordinate CA): This is a CA that uses a root certificate from the main CA to sign its public certificate. Otherwise, it has the same functions as a CA and is also normally named a CA.

A top-level CA must sign its own root certificate and establish trust by the way the certificate is distributed. A Sub-CA can directly establish trust by signing its certificate by the CA's root certificate. Having a number of sub-CAs can also be used to increase trust in the CA as one can compare the signature in the various sub-CA certificates to determine that the same CA certificate has been used by all.

A sub-CA is called a national CA in [16] and it can be operated by a flag state, but also by some regional authority or a third party. Hence the term sub-CA in this document.

Abbreviations

AIS	Automatic Identification system, using a digital communication channel for direct ship-to-ship or ship-to-shore communication at low bandwidths.
ASM	Application Specific Message in AIS or in dedicated ASM channels in VDES
CA	Certificate authority
DMZ	De-Militarized Zone (between two firewalls in computer networks).
GISIS	Global Integrated Shipping Information System [15]
GNSS	Global Satellite Positioning System (examples are GPS, GLONASS, GALILEO)
GS1	Standardization organization for product and location codes [6]
IALA	International association of aids to navigation and lighthouse authorities [7]
IHO	International Hydrographic Organization [8]
IMO	International Maritime Organization, https://www.imo.org/
ISO	International Organization for Standardization, https://www.iso.org/home.html
ISTS	Intelligent Ship Transport System (project), http://ists.mits-forum.org/
IT	Information Technology (network)
ITU	International Telecommunication Union
KSI	Keyless signature infrastructure
MASS	Maritime Autonomous Surface Ships
MSI	Maritime Safety Information
MSW	Maritime Single Window
MRS	Mandatory ship Reporting System (often implemented in a VTS station)
OT	Operational Technology (network)
PC	Personal Computer
PKI	Public Key Infrastructure
RO	Recognized Organization
ROC	Remote Operations Centre (for ships)
S-100	The new IHO system for description and transmission of electronic charts and overlays
SRS	Ship Reporting System (same as MRS)
URL	Universal Resource Locator (normally a web address)
VDE	High bandwidth (up to ca 300 kilobits per second) channel in VDES.
VDES	VHF Data Exchange System: New digital communication system with substantially higher bandwidth than AIS.

VHF	Very Hight Frequency radio (between 156 and 174 MHz for maritime)
VTS	Vessel Traffic Service
XML	Extensible Markup Language

1 Introduction and background

1.1 Scope

Increasing digitalization increases the possibilities for cyber-attacks. This applies to system on the ship and shore, but it also applies to data communication between ship and shore or between ships. This document covers the latter aspect: Securing communication.

The purpose of this document is to outline how an international maritime PKI can be designed and operated. It is based on a report from the CySiMS project [16] but simplified for less technically oriented readers. More technical details can be found in the original report, or in [17] where a requirements and technical analysis can be found.

This report will also look at some of the reasons why digital signatures are needed and what restrictions apply to a PKI that is going to be operated for the international shipping community.

1.2 Background for the report

Over the years, there has been several input papers to IMO on the usefulness and the requirements for digital signatures in digital transactions involving ship certificates or reporting, see, e.g. [1]-[4]. In 2022, this contributed to the publication of the FAL circular "Guidelines on authentication, integrity and confidentiality of information exchanges via maritime single windows and related services" [5]. The circular explains why digital certificates are necessary and how they can be used in single windows and related services. However, it does not address where these signatures are coming from and how they are managed. Thus, this report takes up the thread from the circular and proposes how an international maritime PKI can be designed and operated.

This report is produced by the ISTS project. ISTS covered general digitalization of ship transport, and one of the recognized issues was the need for digital signatures and an international maritime PKI. Much of the technical groundwork was already done by the CySiMS project [16], [17] and a national demonstrator had already been performed in CySiMS SE [18]. This means that most of the technical parts are in place and that the main remaining piece of work is to work with IMO and member states towards a solution that is acceptable to the maritime community. Such a consensus building process may results in some changes to the original CySiMS concept, so it was decided not to do further technical developments before the consensus process was under way.

This document is intended as a first roadmap towards the establishment of the international maritime PKI.

1.3 Structure of this report

This report is structed as follows:

1. This is the general introduction and overview.
2. Some basic information about cryptographic signatures.
3. Some use cases for digital signatures.
4. Restrictions that may make it necessary to create a dedicated maritime PKI.

5. A proposed design for the maritime PKI.
6. Some issues that apply to the use of private signature keys on the ship.

2 Some basics on cryptography, signatures and certificates

2.1 Integrity, authenticity, confidentiality and non-repudiation

When transmitting information in digital format, one faces many risks in that hostile parties can modify information, can send information that they claim are from others or can eavesdrop on information that are intended for others. To avoid such problems, one can use cryptographic technology to protect the data and provide the following functions:

- **Integrity:** A digital signature can be generated so that any change to the data package after signing makes the signature invalid. This makes it impossible to tamper with the content.
- **Authenticity:** By using a digital signature certificate, one can verify the identity of the sender by its signature. The certificate must be issued by a trusted party.
- **Confidentiality:** The technology can be used to encrypt the content if desired. This can be done directly with the key associated with a certificate but will often involve a slightly more complex process to provide better efficiency for larger data sets.
- **Non-repudiation**: By sending an acknowledgement on the received data back to the sender, both sender and receiver can prove that the data was sent. The integrity mechanism will ensure that the content cannot be tampered with or denied being transmitted, by any of the parties. The authenticity mechanisms will prove the identity of the sender and the receiver.

Also, technical problems can change or delete content of a digital messages. To detect such problems, the integrity mechanism can be used. However, if authenticity is not required, a simpler hash function will provide equivalent detection capabilities.

The above are the main mechanisms that are needed to implement a safe, secure and trusted data exchange system [5].

2.2 Public-key cryptography

Public key cryptography is the most common technology used for digital signatures. It includes the use of two keys; a private key, which must remain a secret, and a public key, which can be shared widely. Key pairs are generated with cryptographic algorithms based on mathematical problems termed one-way functions so that one cannot derive the private key from the public. These two keys, which are referred to as an asymmetric key pair, are used to decrypt and encrypt data and to sign and verify digital signatures. Public key cryptography can be used to provide authentication, integrity, confidentiality and non-repudiation of data transfers. This is illustrated in Figure 1 where a hash function is used to calculate a unique hash code over the data to be transmitted. The hash function is specified and known but has the property that it is extremely difficult to generate a new data set that matches a given hash. The hash code is encrypted with the private key and is added to the data as a signature before transmission.

Knowing the identity of the sender and receiving the data file and the signature, the receiver can then use the public key to decrypt the signature and then compare the result with the hash, as calculated by the receiver with the known hash function.

A great advantage of public key cryptography is the ability for one entity to use the same key pair with many other entities rather than having to use a different key with each individual entity. This simplifies the key management process when many different entities, which do not know each other in advance, need to communicate securely. To distribute the public keys, one relies on digital certificates, which bind a public key of an entity to the identity of that particular entity. The entity can be a user, a computer, a service or virtually any other device.

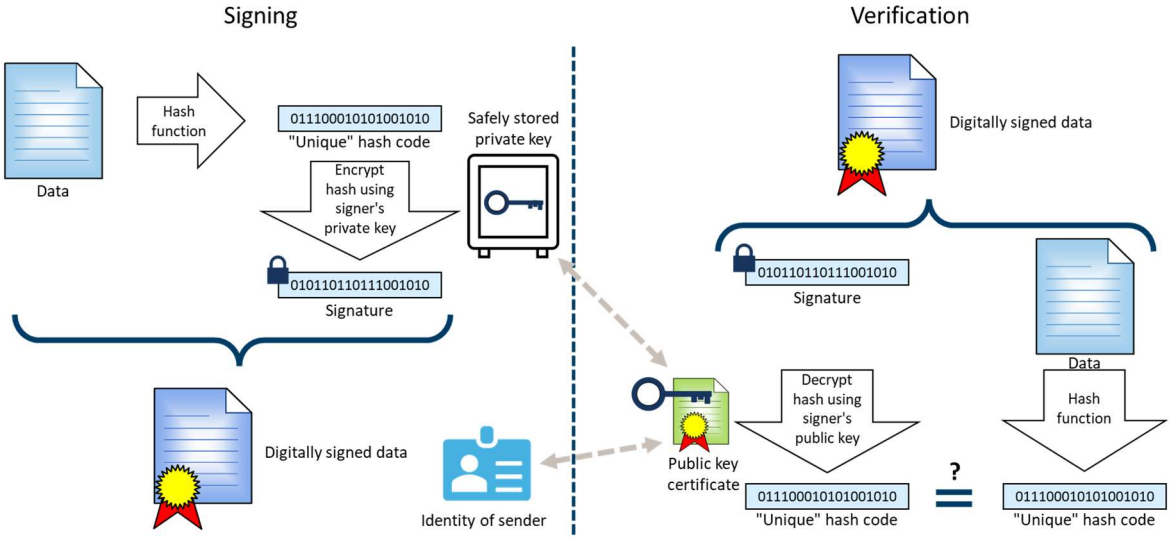

Figure 1 – The process used to generate and verify digital signatures

The proof of authenticity is normally created through a hierarchy of trusted parties, where the top node, the root certificate authority, is an entity that everybody in the system trusts. All certificates, except the root, are signed by a higher authority in the tree and trust in each certificate is inherited down through the tree structure as illustrated in Figure 2.

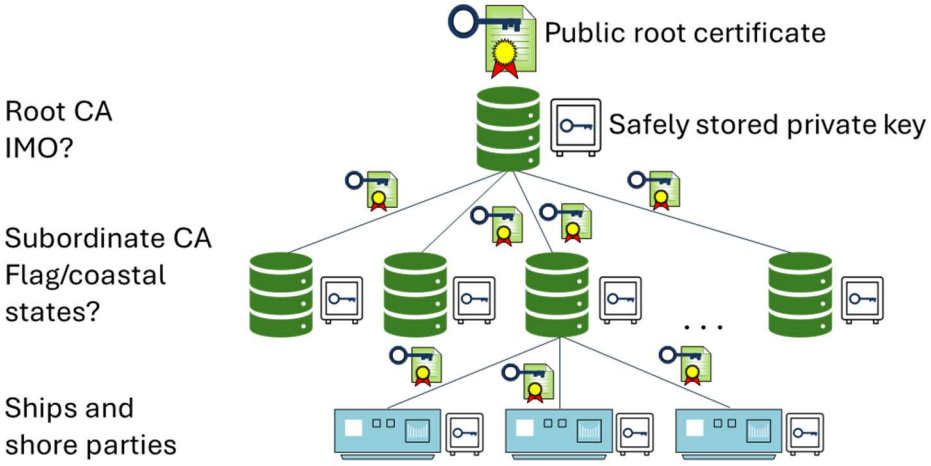

Figure 2 – A public-private PKI hierarchy

For maritime applications one could, e.g. have IMO as the root certificate authority and national authorities as subordinate CAs. This could be, e.g. flag or coastal state authorities or some private company operating on behalf of the national authorities. Several national authorities could also cooperate to set up a common subordinate CA. The trust chain will in all cases be ensured by a common and agreed on root certificate.

Normally, the different certificate authorities will provide a public database with a list of certificates issued by that CA as well as revocation lists and other information necessary to securely use the system. Each of the parties will have a secretly stored private key to match the certificate. The private key is used to sign outgoing messages.

2.3 Blockchain

A blockchain is a distributed ledger with a list of records (blocks) that are securely linked together via cryptographic mechanisms similar to signatures as discussed in section 2.1. Each block contains a signature for the previous block, a timestamp, and additional data related to the transaction that was recorded.

Since each block contains information about the previous block, they effectively form a chain, with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks [9].

The best known blockchains, such as bitcoin, rely on a distributed method for signing each block without any central authority to verify the authenticity of the signer. This is computationally very expensive and is generally a slow process. It also cannot provide authenticity, which is a necessity for maritime use.

However, there are also private or consortium blockchains that use the same ledger principle with irreversible recording of transactions. Here, one or more accepted authorities provide certificates for signing which can also provide authenticity checks for the signers. The benefits of these blockchains are partly a computationally cost similar to ordinary cryptographic methods, partly that consortium blockchains can require that all authorities agree before a record is added, and partly that they provide an unmodifiable history of transactions. This is useful in certain contexts such as when one needs to control the proof of ownership in complex trade processes. Examples are a ship certificate during the building, approval, payment and hand over phases, or for negotiable bills of lading. However, for most applications as discussed in section 3, public-private cryptography is preferred [10].

Public blockchains have the drawback that all transaction records must be available and readable for the public. This is often not desirable and may disqualify blockchains as a trust building mechanism.

2.4 Other cryptographic technologies

Self-sovereign identity (SSI) is based on blockchain technology and implements an identity management system that is independent of a centralized certificate authority [12]. The drawback of this system is that trust must be established through direct knowledge of the other party, i.e. there is no common trusted party that links the identity code to a specific legal party.

Private and consortium blockchains need more control over who adds entries to the ledger. An alternative to the conventional blockchain methods for adding entries is the keyless signature infrastructure (KSI) [11]. It uses a tree structure of hashes of hashes over several documents to avoid that one document can be changed without changing the whole tree. Thus, KSI has similar properties as blockchains without needing asymmetric key sets as in private-public cryptography.

KSI will, as blockchains, not provide authentication of the signer. Thus, it is of limited interest in the scope of a maritime PKI.

2.5 Secure transmissions versus signed messages

Most data transmissions today will be done over secured connections which normally use the same public-key cryptography mechanisms as discussed in section 2.2. This is transparent to the user as the systems use standardized and internet available certificates to establish the secure data link. This will satisfy some confidentiality and integrity requirements. It will not in itself be able to establish the identity of the sender, although the receiver may be authenticated with a certain level of confidence, dependent on who issued the receiver's certificate (see section 2.9).

These mechanisms will not be sufficient to ensure non-repudiation, and its use depends on both sender and receiver residing live on the internet so that the relevant certificates can be retrieved and validated. These mechanisms may be somewhat easier to break, e.g. by cyber-attacks of the man-in-the-middle type, than end-to-end signing and/or encryption of messages.

For ships using, e.g. VDES to communicate between themselves without having internet access, other mechanisms are needed. This is also the case for communications that require secure identification of sender and receiver, and if non-repudiation is needed. This document proposes a PKI also for these types of applications.

2.6 Authenticating access to API access points

One may also need to authenticate physical parties before they are granted access to certain APIs or API access points. If implemented, this will normally involve the use of a special authorization API as illustrated in Figure 3.

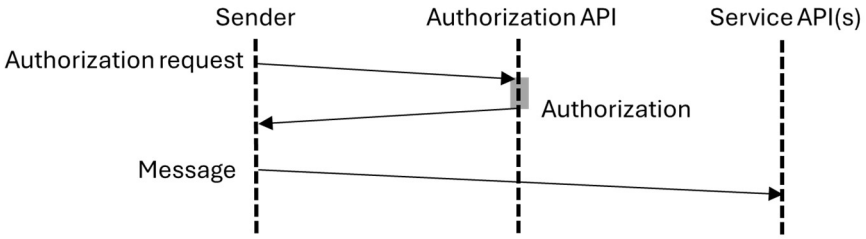

Figure 3 – Access authorization

The authorization message will contain an authorization code that is used on subsequent calls on the service APIs.

The authorization call can use digital signatures to verify the identity of the sender. Calls to the service APIs will not require authentication by digital signatures, but digital signatures for integrity checks and non-repudiation may still be necessary.

2.7 Securing a communication link between known parties

In some cases, e.g. for communication between MASS and ROC (see section 3.4), one will set up a secure communication link between two mutually known parties. This will not require a general digital certificate mechanism as the two sites directly can agree on how the communication link shall be secured. It may be convenient to use a public key certificate, but it is not necessary.

2.8 Special considerations for VDES data exchanges

The automatic identification system (AIS) is a well-known communication channel for automatic transmission of ship position and movements between ships and from ship to shore or satellite. It also has facilities for sending more general binary messages, so-called application specific messages (ASM). However, the coexistence between ASM and the more conventional AIS messages is becoming a problem as bandwidth is limited in the two established main AIS channels. Thus, the VHF Data Exchange System (VDES) has been proposed to better support the diverse applications for shorter digital messages between ships and between ship and shore. VDES is not yet a carriage requirement for SOLAS ships, but IMO and IEC have now started work on new performance and test standards.

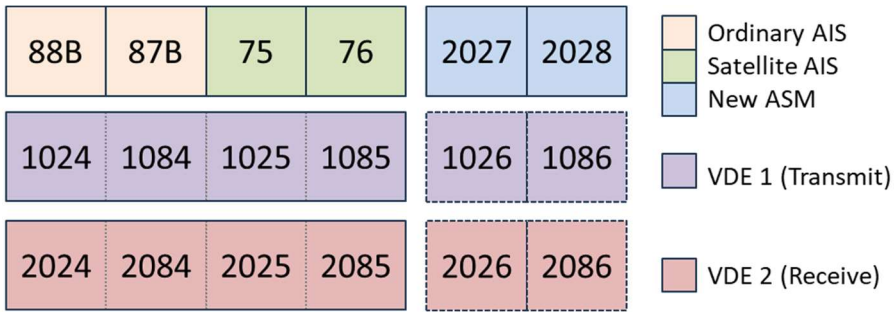

Figure 4 – VDES Channel allocation

VDES will incorporate the existing AIS system as illustrated in Figure 4, including the two long range AIS channels used for space segment reception of AIS messages. VDES will also implement several new and higher capacity radio channels. Two new ASM channels provide approximately double the capacity of an AIS channel each, and is intended to be used for ASM messages that are today transmitted on the ordinary AIS channels. One concurrently transmit and receive high capacity VDE channel, each using up to four 25 kHz VHF channels, can support from around 38 to 300 kilobits per second data transmissions for new and more advanced digital data transfers. Additional VHF channels are allocated to avoid cross-talk between VDE and other VHF channels.

Although VDE can be used for data streaming, it is expected that most or all transmissions would be message oriented, e.g. as a delimited S-100 type message or similar. AIS and ASM channels will always be message oriented.

VDE is expected to be used for safety critical data exchanges independent of the ships having access the internet. As safety requires authentication and integrity checks, the implementation of VDES will require a digital signature system that can operate without internet access. It may also be necessary to encrypt some messages if they contain sensitive data. VDES messages can be received by any party that has a suitable radio receiver.

Note also that the scheduling of VDES system messages uses a special bulletin board mechanism that is defined in the VDES specification [13]. ITU has already given these messages space for a digital signature, but the PKI has not been defined.

2.9 Level of trust in a certificate

The trust one can have in a certificate is in part based on the trust one has in the certificate authority and in part by the process the CA uses to determine the identity of entities that it issues

certificates to. There are three different processes in common use with increasingly reliable verification measures:

1. *Domain validation (DV):* This verifies that the party the certificate was issued to also has control over the internet domains the certificate covers. This is typically used for securing internet connections to web platforms using HTTPS and normally uses an automated and simple test procedure to verify control over the internet domains.
2. *Organization validation (OV):* In addition to the domain validation, this certificate also may prove the organization's actual existence as a legal entity. This can be based on an automated process that may be susceptible to forgery.
3. *Extended validation (EV):* This extends the organization validation by stronger proof of the organization's actual existence as a legal entity, including manual verification by a human.

For use in international shipping an EV level certificate is a minimum requirement. The trust in the CA and its capabilities must also be ensured.

3 Why do we need digital signatures?

3.1 Introduction

As explained in section 2.1, digital signatures can provide checks for integrity or authenticity. They can be used to encrypt information for confidentiality and, together with acknowledgement, can be used to implement non-repudiation mechanisms.

Section 2.5 also discussed the use of secure transmission as a replacement for integrity and authenticity checks in the message itself. However, this will depend on having sufficient trust in the holder of the certificate used to establish the secure transmission. The level of trust was discussed in section 2.9.

This section will give some general examples of where such mechanisms may be needed and what type of mechanisms that can be used. This is not an exhaustive list of applications.

3.2 Human readable documentation

Even when the intended recipient of an electronic document is a human and one assumes that the human will do certain sanity checks on the document before using its content, digital signatures are important to verify that the sender really was the one it claims to be and that the content has not been tampered with.

If this is not in place, it is easy to falsify, e.g. electronic charts to change depth contours and make the ship sail onto a reef or similar. This problem applies to all documents that have some safety aspect related to it.

Safety related of information should contain authenticity and integrity signatures. Alternatively, the information may also be transmitted over a secure data link from a trusted source.

3.3 External data for automation systems

An even more critical situation is when the received data is not used by a human but used directly in an automated operation. It is possible to build some sanity checks into the automation systems, but it is also feasible to provide falsified data that is not detected by the automation.

A good example is AIS where it is trivial to spoof messages and give false information to nearby ships. Thus, it is obvious that AIS cannot be used in automated and safety related functions. For GNSS, there is a similar problem, although spoofing is somewhat more complicated. Neither GNSS or AIS have enough bandwidth to use digital signatures, but the coming VDES system has capacity in larger ASM messages and in the VDE channel that may be used to also secure this type of information.

If this type of information is to be used in safety related automatic control, authenticity and integrity signatures are required. Alternatively, the information may also be transmitted over a secure data link from a trusted source.

3.4 Autonomous ships – MASS

MASS is a special case of automation where there may be no crew left onboard. Many safety-related functions will be fully automated, but humans will still be needed in the ROC. One reason

for this is that IMO most likely will require that all ships, including MASS, must have a human master and that the master must have the possibility to intervene in the operations of the MASS. Also, it is unlikely that automation will be good enough to reliably be able to handle all situations a ship may encounter. Thus, it will in most cases be most cost effective to use ROC-operators to handle very complex situations rather than building and approving extremely complex automation functions.

This means that MASS will have the same issues as described in section 3.3 with regards to digital input to the automation system. In addition, a MASS also needs secure communication between the ship and its ROC.

However, the communication between MASS and ROC may go through dedicated and secure communication links that are set up between parties known to each other. Thus, there may not be a need for general digital certificates to secure this communication link (see section 2.7).

3.5 Crew or ship certificates, bills of lading and similar

Crew or ship related certificates will be held by the crew member or the ship's management but will have been issued by another party.

Similarly, certain documents related to the cargo, e.g. a bill of lading or various safety certificates, may also be carried onboard while having been issued by another party.

To verify validity of this type of document, the document itself needs to be signed by the issuer. This will establish the authenticity of the document and that it was not tampered with.

A secure transmission can be used to transfer the document, but this must be established from the issuer of the document or another trusted party.

3.6 Mandatory reporting – MSW

Mandatory reporting systems, e.g. a maritime single window, may be mandated by national legislation, where failure to report or where errors in reporting may have criminal or commercial consequences. Thus, message exchanges should ensure that both parties can prove that the message exchange took place and that the content of the message can be reestablished.

Mandatory systems will normally be operated by national authorities and should not in general need confidentiality beyond general protection of data in transit.

All such reporting should be associated with digital signatures and acknowledgement mechanisms that implement non-repudiation.

3.7 Port service systems – PCS

Some public systems, e.g. a port community system, are similar to mandatory reporting systems, but are normally operated under commercial agreements rather than national legislation. They are usually operated by independent third-party commercial entities. They will have similar requirements regarding signatures as an MSW but may in addition require that certain data is protected by encryption. This may, e.g. be health or personal data that should be protected from access by the third-party PCS operators.

These public data exchanges may imply commercial liability and will as a rule require mechanisms for non-repudiation.

3.8 Commercial services

It is also relevant for the ship to order certain services in a port from other parties, e.g. bunkers or food supplies, that may have commercial consequences if not used or if arrival times changes.

In such cases, all orders, changes or cancellations should be associated with digital signatures and acknowledgement mechanisms that also implement non-repudiation.

However, in these cases the parties may enter into some form of commercial contract before the service is provided and this can be used to exchange the appropriate public key certificates. Thus, it may not be necessary to have a general maritime PKI.

4 Restrictions that apply for an international shipping PKI

4.1 Introduction

As discussed in section 3, for many types of maritime digital communication, a digital signature will be required. If this is going to be a general mechanism for international shipping, one will also need an internationally recognized PKI. However, international shipping poses some challenges that do not apply for most other PKIs. This section describes these challenges.

The main problem facing international shipping is the identity and authentication of the parties. As ships travel all over the world and need a more reliable authentication than what is available for common international services, one needs a reliable identity management scheme that can work across state borders. Some of the communication types and associated identity authentication issues are illustrated in Figure 5. The arrows are coded as indicated at the bottom. Dashed lines, where used, indicate optional connections. The figure is not exhaustive but provides typical examples.

The left-most column shows typical land-based parties associated with an international port call. The middle column illustrates the ship, its foreign associates as well as certification authorities. The right-most column is typical nautical parties encountered during the voyage and port approach.

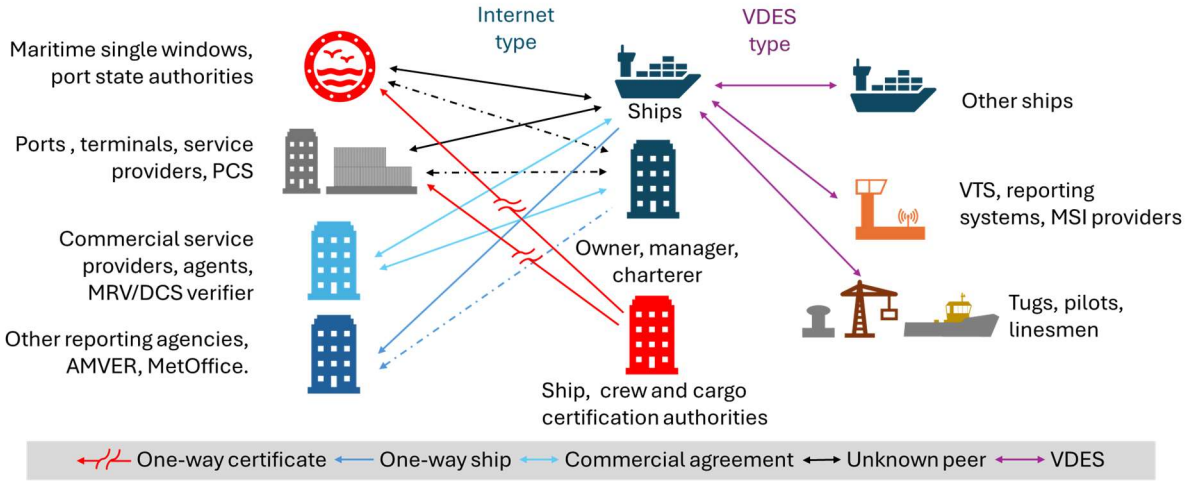

Figure 5 – Overview of ship specific PKI requirements

The main differences between the cases are in how identity needs to be authenticated:

1. *One way certificate*: In this case a crew or ship certificate is issued by some international authority. The certificate is then transferred from the holder to some other party to prove that the holder has the capabilities specified in the document. The identity and of the authenticity of the authority need to be assured by a digital signature on the certificate.
2. *One way ship:* This is typically some report that is sent by the ship to a reporting service. The identity and authenticity of the destination will not be critical to safety. The identity and authenticity of the sender may be critical for legal or commercial causes. Thus, a digital signature should be added to the report. Note that non-repudiation may be needed if failure to send report has legal or economic consequences.

3. *Commercial agreement:* There is an existing contractual agreement between sender and receiver that will help to assure identity and authenticity of both parties. One may not need an international PKI, but that would simplify authentication of parties.
4. *Unknown peer:* This is a communication between two parties that are not necessarily known to each other. Identity and authenticity of both parties must be ensured by digital signatures.
5. *VDES:* This is the same as the unknown peer case, but over a data link that can be operated without internet access. Thus, identity and authentication must be established without internet access.

The following sections will give more background on the identified challenges.

4.2 Internationally recognized

A shipping PKI will be used by foreign flagged ships when calling on international ports. Any shipping PKI should have a status as internationally recognized by all flag and coastal states. This could be arranged by including the acceptance of key certificates and signatures through an amendment to the FAL Convention.

For ships calling in international ports it may also be possible to use a PKI that is established by the flag state of the ship. This would establish a link between the state that has jurisdiction over the ship and the ship itself. The acceptance of this type of PKI should also be included in the FAL Convention.

For ports and other shore parties one could use the same PKI as the ships flagged in that state. It is also less of a legal problem to use a nationally recognized PKI, as the party resides in a specific state and legislation in that state will in any case apply to digital transactions involving that party.

4.3 Internationally recognized identity

Public-private key cryptography will also require that all parties can be identified by an internationally recognized name or code. For ships this could be the IMO number or the MMSI. The benefit of the IMO number is that it is directly connected to the ship. However, MMSI may be more useful as it identifies the radio-communication equipment used by the ship, which is very relevant for VDES transmissions as the sender's MMSI is already included in all messages. MMSI also has the benefit that it changes if the ship changes flag. A change in ownership will normally require the issuance of a new key certificate naming the new owner.

Ports can be identified with, e.g. location codes from the UNECE UN/LOCODE system [14]. Terminals and berths could rely on identification systems developed in other organizations, such as GS1, IALA or IHO.

VTS and reporting systems may also be identified by their MMSI number. The MMSI will The identity of other entities should be agreed on during the development of the PKI.

4.4 Jurisdiction and enforcing liabilities

Another issue related to ships in international trade is to enforce liabilities on the ship when it is outside territorial waters of the state where the liability was incurred. Here, the most straight

forward solution would be to associate the certificate and the digital signature with the flag state as the flag state has jurisdiction over the ship. This would assume that the flag state also is willing to enforce its jurisdiction.

Another, more complex solution would be to issue certificates through IMO and amend the FAL convention to say that flag states shall recognize liabilities incurred by the ship through its use of digital signatures.

One could also envisage commercial organisations where ships, e.g. deposited or guaranteed for a certain amount through the organization that issued the certificate. However, with more than 100 000 ships in international trade and 176 different member states in IMO, this would lead to a complicated set of contracts and agreements.

4.5 Ships are not always online

A final problem is that ships may not always have access to internet. Satellite coverage is not necessarily global or constant and equipment problems may occur. This is not a problem for internet-based data transfers as these cannot take place unless there is a connection. However, for VDES this will be an issue. VDES is a dedicated line-of-sight communication channel and will be used, e.g. between ships at sea. This means that ships may exchange messages with each other or with shore installations without having access to internet.

Some of the entities that may use VDES are:

- Other ships. There are around 150 000 ships in international traffic world-wide. Approximately 350 000 if all ships with IMO-numbers are included.
- VTS and MRS in the coastal state areas, including port VTS and similar. This is a limited number and probably well under 10 for most coastal states. As an example, USA operates 12 VTS stations. Norway has 7 VTS station, including the information service for the Barents SRS. Each VTS should have its own identity.
- MSI broadcasts. This is also limited to a few stations in each coastal area. Each should have its own identity.
- Ship service resources in the port approach area, e.g. tugs, terminals, port authorities etc. This is also a limited number and service providers in the same port may share the same identity.

Other entities like MSW, PCS, terminal and port management systems are expected to communicate via internet protocols. VDES has limited bandwidth and is most useful for real-time and line of sight communication.

Note that VDES also has provisions for communication via satellite. This probably have a limited number of business cases, as satellite bandwidth is expected to be significantly lower than ship to ship communication.

Ships using VDES or other similar communication mechanisms and which are interested in checking authenticity of data received from shore or another ship should cache relevant digital certificates before commencing on a voyage. In some cases, one could also include the certificate in the messages and make sure that the root CA was known and trusted by all parties in the

maritime domain. However, for VDES, this would require more bandwidth and may not be a suitable solution in all cases.

5 A proposed design for an international maritime PKI

5.1 Introduction

There are several ways to arrange a maritime PKI as discussed in previous sections. There are two possibilities that seem reasonable:

1. One centralized PKI for all maritime users with one common root certificate. This could be administered by IMO or delegated to a commercial operator. However, it is not likely that all states will agree to this, and the complexity of the setup would be relatively high.
2. A more realistic proposal is to delegate the issuance of national certificates to the flag state, or another operator authorized by the flag state. This could also be a regional solution where several states work together. Here, each state would be a CA and could have a certificate signed by IMO to be used as a common trust anchor.

Having several national PKIs, all with the same root certificate authority signing their respective certificates, would also give some confidence that the common root certificate has not been falsified. For the central authority, e.g. IMO, it would only need to issue some 180 certificates, so building very strict security protocols into the central management should be feasible.

As was discussed in section 4.5, the entities that are most important to cover in a maritime PKI are the ships themselves as well as shore entities the ships may contact using VDES. The latter entities are also those that the ship itself most commonly would contact using internet protocols and having them in the same PKI would be useful for faster and safer lookup.

General commercial entities can in principle use the maritime PKI but can also use other nationally recognized certificate authorities. It will be up to the administrator of the PKI what entities to allow to register.

5.2 A three-layer PKI

Based on the above discussion one can illustrate a three-layer PKI as in Figure 6. The flags are arbitrary and is used to illustrate different flag states.

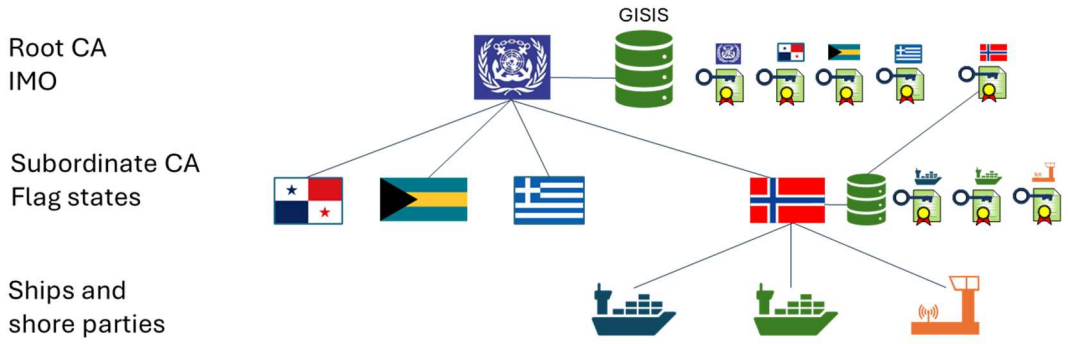

Figure 6 – A three-layer PKI with IMO as CA

IMO is the primary CA while flag states operate their own national certification authorities. It is suggested that all flag state certificates are available in GISIS together with the URI for their national list of public certificates. This makes it easy for ships to read and cache at least the flag state certificates. It would also be possible to read and cache the certificates of ships in the

national databases as that would enable immediate authentication of the signature of all relevant parties. This is mostly of interest for VDES users that do not have access to internet.

Thus, the general requirements to a maritime PKI should be:

1. A ship's certificate should be linked to a ship's flag state. This will be achieved in this setup.
2. Ships should have certificates in the PKI hierarchy directly below the flag state, i.e. a three-layer PKI.
3. All national authorities should use IMO or similar organization as CA for own certificate.
4. IMO should publish the national authorities' certificates and an URI for retrieving ships' and other entities' certificates from the national authorities' PKI. This can be done through GISIS [15].

Note that the illustration and discussion do not cover the full functionality of PKIs. It will also be necessary to establish procedures for issuance of certificates, withdrawal of the same and maintenance of revocation lists. Details about this can be found in [16].

6 Ship-side implementation

6.1 Introduction

In addition to general restrictions as discussed in section 4, there are also some more specific restrictions that should be considered when using the digital certificates on ships. Some of these restrictions may also be applicable to some shore-based installations.

6.2 Secure storage of private key on ships

The protection of the private key is essential in all applications of public key cryptography. However, the level of protection will normally vary with the criticality of the application. Thus, for many land-based applications, such as web servers, the private key is stored as a data file on one or more computers that are protected from access by unauthorized personnel. However, a physical attack on the premises or a cyber-attack via internet could make the private key available to unauthorised persons. It may also be difficult to detect that the key has been stolen before some form of forgery with the private key has been committed and detected. For ships, this may be too weak protection for a private key. Ships sails between many different countries and change crew at regular intervals. There may also be service personnel onboard.

Thus, a more appropriate protection would be to embed the private key in a special device or a smart card that also performs the cryptographic transformation of the signature. It will not be possible to steal the key without also stealing the device or the smart card. By physically limiting access to the card or the device, this would make it more difficult to steal. It is also much easier to detect that the key has been stolen when it cannot be duplicated but requires that the whole card or device is removed.

6.3 Use of protected OT networks on ships

Ships contains numerous networks, both IT and OT types. OT type networks, e.g. the bridge network, needs extensive protection to avoid cyber-attacks on critical ship equipment. However, the bridge network will also need to sign or verify messages, e.g. on VDES. Many of the reporting and shore communication systems will reside on IT networks. Thus, any digital signature mechanism should be accessible from both IT and OT networks. There are several ways to achieve this:

1. Use two (identical) private keys in the two different locations. This may be less desirable as chances for loss of key may be greater and management of keys somewhat more complicated.
2. Use a dedicated signature box that has double Ethernet connections, one to the IT and one to the OT network. One should use a dedicated box in this setup to minimize chances that, e.g. a general PC connected to the OT network gets infected by virus or are otherwise used in a cyber-attack on the OT network and devices.
3. It is also possible to use one signature PC or box placed an a DMZ between the OT and IT networks. IEC 61162-460 [19] has specifications for how such a setup should be implemented.

For best safety and security levels, a dedicated signature box from a reputable manufacturer is the preferred choice.

6.4 Caching of certificates

If VDES is used without access to internet, the ship needs to cache certificates for relevant entities. There are several options:

1. Caching only the top-level CA certificate. This requires an exchange of all intermediate certificates as well as the other ship's certificate before secure communication can commence. This amounts to two certificates if a three-level PKI is used.
2. Cache the intermediate CA certificates. This is approximately 180 certificates, one from each of the relevant flag states. This only requires exchange of the other ship's certificate before staring communication, i.e. one certificate.
3. Cache certificates from all ships, VTS and reporting systems. This avoids exchanges of certificates and, thus, saves bandwidth. This will require the caching of some 200 000 certificates.

VDES has limited bandwidth, and this must be considered against the cost of caching certificates. A certificate varies in length but is typically around 500 to 600 bytes in binary format. This may be reduced if more compact identity codes are used.

Caching may also cause problems with invalid certificates unless proper routines for checking validity of certificates are implemented.

References

[1] IMO FAL 39/5/2, e-business possibilities for the facilitation of maritime traffic, Technical standards for implementing electronic certificates, Submitted by ISO, 10 July 2014

[2] IMO FAL 40/6/2, requirements for access to, or electronic versions of, certificates and documents, including record books required to be carried on ships, Future Proof and Cost Effective Standardization of Electronic Ship Certificates, Submitted by ISO, 21 December 2015.

[3] IMO FAL 41/5/3, application of single-window concept, Comment on the agenda item on Application of Single-Window Concept, Submitted by ISO, 8 February 2017.

[4] IMO FAL 43/8, developing guidance for authentication, integrity and confidentiality of content for the purpose of exchange of electronic information, Proposal for guidelines for authentication, integrity and confidentiality of content for the purpose of exchange of electronic information, Submitted by ISO, 20 December 2018.

[5] IMO FAL.5/Circ.46, Guidelines on authentication, integrity and confidentiality of information exchanges via maritime single windows and related services, 1 June 2022

[6] GS1: https://www.gs1.org/

[7] IALA: https://www.iala-aism.org

[8] IHO: https://iho.int/

[9] Wikipedia article on Blockchain: https://en.wikipedia.org/wiki/Blockchain

[10] Rødseth, Ø. J., Meland, P. H., Frøystad, C., & Drugan, O. V. (2019). PKI vs. Blockchain when Securing Maritime Operations. *European Journal of Navigation*.

[11] Buldas, A., Kroonmaa, A., & *Laanoja*, R. (2013). Keyless signatures' infrastructure: How to build global distributed hash-trees. In *Nordic Conference on Secure IT Systems* (pp. 313-320). Berlin, Heidelberg: Springer Berlin Heidelberg.

[12] Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80-86.

[13] Recommendation ITU-R M.2092-1 (02/2022), Technical characteristics for a VHF data exchange system in the VHF maritime mobile band.

[14] UNECE UN/LOCODE: https://unece.org/trade/cefact/unlocode-code-list-country-and-territory

[15] Global International Shipping Information System: https://gisis.imo.org/Public/Default.aspx

[16] CySiMS Report D2.2: Using digital signatures in the maritime domain, March 2017, https://ists.mits-forum.org/resources.html#H6

[17] CySiMS report D2.1 Digital signatures for nautical use: Analysis of requirements and possible solutions for an international maritime Public Key Infrastructure (PKI). https://ists.mits-forum.org/resources.html#H6

[18] Presentation of the CySiMS demonstration: https://97417a95-6c5a-4028-a47d-5e96784b7edf.filesusr.com/ugd/fe2404_bfc0c3e980f9424aa08b9e43a57fb241.ppsx?dn=cysims-se-short_audioPres.ppsx

[19] IEC 61162-460, Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security