IOP Conference Series: Materials Science and Engineering

PAPER • **OPEN ACCESS**

The need for a public key infrastructure for automated and autonomous ships

To cite this article: Ørnulf Jan Rødseth *et al* 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **929** 012017

View the article online for updates and enhancements.

This content was downloaded from IP address 129.241.231.175 on 21/01/2021 at 11:19

IOP Conf. Series: Materials Science and Engineering **929** (2020) 012017 doi:10.1088/1757-899X/929/1/012017

The need for a public key infrastructure for automated and autonomous ships

Ørnulf Jan Rødseth[1,*], Christian Frøystad[2], Per Håkon Meland[2,3], Karin Bernsmed[2], Dag Atle Nesheim[1]

[1]SINTEF Ocean, Trondheim, Norway
[2]SINTEF Digital, Trondheim, Norway
[3]Norwegian University of Science and Technology, Trondheim, Norway

[*]E-mail: OrnulfJan.Rodseth@sintef.no

Abstract. Shipping undergoes rapid digitization, covering safety and security reporting, mandatory ship documentation, electronic port clearance as well as commercial and operational information exchanges. Increasing automation of information processing, including the specific needs for autonomous ships, requires increased "digital trust" to allow humans to remove themselves from the information processing loops. This includes better safeguards against cyber threats such as counterfeiting contents or the originator of critical messages. This paper describes thirteen use cases for maritime services and analyse how a Public Key Infrastructure (PKI) system can provide security barriers to mitigate relevant cyber threats and possible consequences of unwanted events. Such a PKI needs to be designed with the special maritime business constrains in mind; the most important being the international nature of shipping, the lack of connectivity for ships that are far from shore, the network constraints associated with existing communication technologies and regulatory considerations.

1. Introduction

Today, maritime shipping undergoes rapid digitization. This applies to safety and security reporting, mandatory ship documentation, including ship certificates, electronic port clearance as well as commercial and operational information exchanges. There are at least two important reasons for introducing digital information exchanges in the conventional maritime sector. One is to reduce the administrative workload on the involved parties, most importantly the seafarers. This can be done by using computers to automate the processes related to the information transmission, reception, and processing. The second reason is to improve the quality of information used to plan and execute maritime and port operations. Electronic transmissions avoid misunderstandings and simplify the exchange of more complex information. However, even when we assume that electronic communication is error free, there are three issues with this type of data exchange that need to be addressed: One is the possibility of malicious cyber-attacks that may be motivated by commercial gain or attempts to damage life, health, property or the environment or are just random attempts to break into interesting technical systems. The second issue is to establish enough trust in the automated processes so that the need for manual double checks is reduced to a minimum. If not, administrative workload may increase rather than being reduced. A third issue emerges when

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

ships become more automated and eventually without people onboard. This removes the human from the information evaluation and decision-making process, and it becomes critically important to ensure that the digital information is correct and that it can be trusted.

Problems occur if the *safety and security mechanisms* that are inherent in the document-based systems are not replicated and improved in the electronic information exchanges. These mechanisms are:

- *Confidentiality* (sealed and closed envelope): the contents of the document cannot be read by others than the intended receiver(s).
- *Integrity* (broken seal, changes to the printed paper): document tampering will be detected.
- *Authenticity* (signatures, stamps, seals): the identity of the originator of the document can be proven.
- *Availability* (archives, delivery): The document can be easily transmitted, found, and retrieved within a reasonable amount of time.

In addition, an additional mechanism can be derived from the three above, which is *non-repudiation* (registered mail, courier): providing proof that the document was delivered to the recipient, which generally requires an authenticated acknowledgement from the receiver that the specific document has been received.

There is a diverse set of communication interactions in shipping, including ship-to-ship, ship-to- port, ship-to-Remote Control Centre (RCC), ship-to-Vessel Traffic Services (VTS), ship-to-Application Service Provider (ASP), ship-to-Medical Aid Provider (MAP), and ship-to-Search and Rescue (SAR) as well as ship to Maritime Rescue Coordination Centre (MRCC), see Figure 1. The communication directly between the ships and between ships certain land services are likely to be VDES (orange), while other communication between ship and shore might be SatCom (blue). Satellites can be in Low or Geostationary Earth Orbit (LEO or GEO) and communicate via a Satellite Application Service (SAS), to shore entities over land lines (green). GEO-solutions are normally Very Small Aperture Terminal systems (VSAT, i.e. directional dish antenna), but can also be low- directional services such as some of Inmarsat's services. The most common LEO-service today is Iridium, but there are also satellites available that can receive and send VHF digital data. Much of this communication is today done with via Very High Frequency (VHF) voice radio or Satellite Communication (SatCom) telephone links.

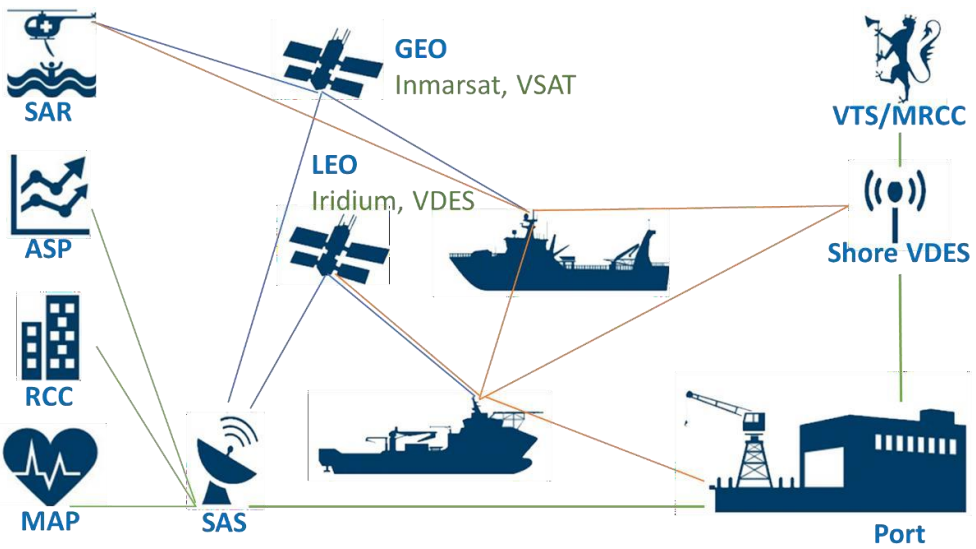

Figure 1. A high-level overview of some communication channels between maritime entities.

VHF Data Exchange System (VDES) [1] is a new two-way radio communication system, which is currently being standardized and validated for various maritime services. By transitioning from

analogue voice to digital messages over VDES and making more use of Internet based exchanges over SatCom, the stress on the current communication links will be reduced and new services can be introduced. The use of the different communication links will depend on the ship's location, information to be transmitted, and the stage of the ship's journey. The digital data exchanges need to implement a digital trust model, and the use of a Public Key Infrastructure (PKI) is a common way of realising this. However, with every PKI there are several design and configuration decisions that must be made based on the nature of the operating environment. There are distinct characteristics for this domain that must be taken into consideration for a PKI to be economically, technically, and politically feasible. This paper will elaborate on the business constraints underlying a PKI for the maritime industry and discuss PKI related solutions and initiatives used in a maritime setting. We will use a selection of business cases for maritime digital communication based on the following three groups of ship communication needs:

- Safety related communication over VDES, to other ships or to shore.
- Internet message exchanges associated with the Maritime Single Window [2].
- Commercial and operational services, mainly over SatCom and Internet.

In section 5.1 we present thirteen use cases related to these and continue with an analysis of possible unwanted events caused by cyber threats and possible consequences. We then suggest how a PKI can be used to create barriers for unwanted events related to the use cases.

2. PKI basics

One of the most common technologies to provide secure and trusted digital data exchanges is the use of Public Key Infrastructure (PKI). A functioning PKI solution needs to be able to create, store and distribute cryptographic keys amongst a wide variety of users (including vessels, authorities' shore stations, and organizations) that will need to communicate securely in order to exchange critical information. The PKI can be used for authentication and to establish cryptographic protection of ship-to-shore, shore-to-ship, and ship-to-ship communication, independent of what communication link is being used. The solution can also be used to generate and validate digital signatures of, for example, electronic ship certificates and logbooks.

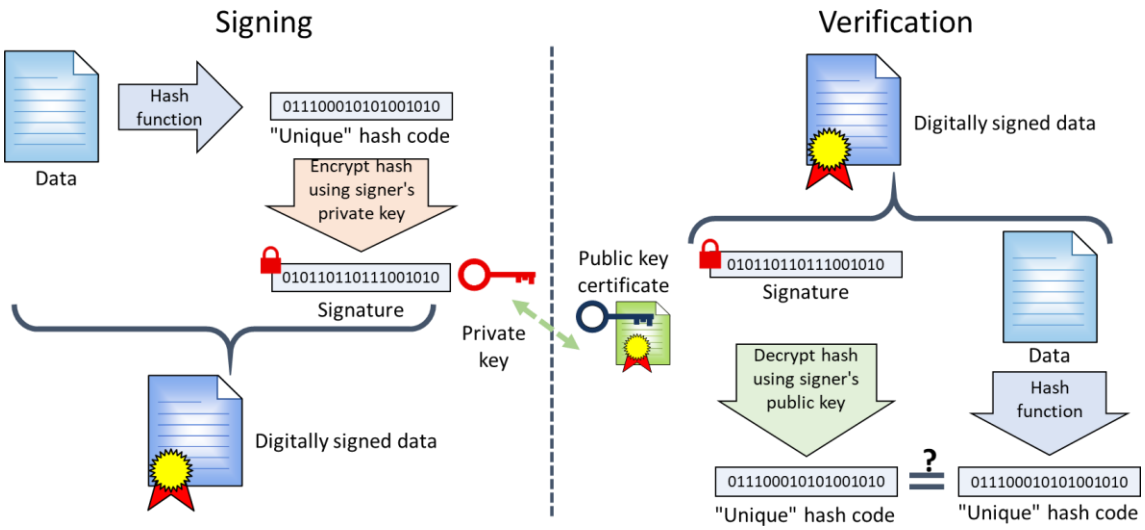

Figure 2. Overview of private/public key basic function

The public-key digital signature mechanism is illustrated in Figure 2, where a securely issued private key and a corresponding public key certificate are the main enabling assets. Once the sending party has digitally signed a message (or document) using his or her private key, the contents of the message can be verified by anyone having a copy of the sending party's public key, which usually is made available in a digital public certificate. The system requires a trusted authority to issue the

public certificate of the signing party. The public certificates enable anyone to verify that documents sent by a private key holder are indeed issued by that party and that the content has not been tampered with.

When both parties are part of the PKI, it is easy to send acknowledgements on reception that can be verified by the original sender and used as proof that the original message was indeed sent and received. The sender's signature on the original message serves as proof of the actual content of the message. This implements non-repudiation.

Encryption (confidentiality) of the message contents can be implemented in different ways, also by using the public/private key mechanism. However, normally one will use other and more efficient mechanisms where the PKI is used to negotiate and exchange symmetric encryption keys. These are further useful for securing vessel services with real-time requirements, such as voice communication, system monitoring and remote piloting. Note that it is also possible to encrypt a message with the public key, so that only the owner of the private key can open it.

3. Maritime business constraints

There are many PKI solutions already in operation all over the world, but the maritime sector has some important business constraints that limits using off-the-shelf solutions. This section will go through the most important of these.

3.1. The international nature of shipping

Ships regularly call on ports in other countries than where they are flagged. Generally, the ship owner, manager or charterer are also located in other nations than where the ship calls. As there is no common legislation covering all the communication parties, it may therefore be difficult to accept messages or reports from ships to shore as legally or commercially binding under national law. It is of course possible for ships to get nationally accepted public certificates, but this may not be legal in some jurisdictions and will also create a management problem for ships that call in ports belonging to different nations.

A related problem occurs when ships meet at sea (international waters) and need to exchange safety related information, or when a ship passes through a ship reporting or VTS area and needs to exchange information with shore stations.

This constraint means that one internationally managed PKI would be useful to simplify management of ship and shore entity certificates.

3.2. Ships are not always connected to the Internet

Not all ships are continuously connected to the Internet as coverage may be very limited far from shore. This condition makes it difficult to use security solutions that rely on constant network access for their functionality. Existing PKI systems we know from the vast World Wide Web, various blockchain implementations and secondary channel solutions (e.g. SMS codes to mobile phones) would typically fall in this category.

However, within the shipping sector there is a limited number of parties that need to be involved, i.e. between 55 000 and 120 000 ships, dependent on how they are counted, and approximately 110 000 registered ports. This makes it possible to load all trusted root certificates for a PKI, and probably all public key certificates as well, onto the ship when it is in port with a high capacity Internet connection. This cache can be used to verify the electronic signatures received during the part of the voyage when it does not have access to the Internet.

3.3. Limited bandwidth and message sizes

Even when ships have a network connection during the voyage, they usually have a relatively low bandwidth and high communication latency. The cost of communication can also be a limiting factor. Also, some of the new e-navigation services is expected to operate over the VDES data links for some of the message exchanges. This has further restrictions in terms of message size and *Quality*

of Service in general (message loss, latency, jitter). These issues have consequences for the cryptographic strength and how the PKI is implemented in practice. One cannot allow large signatures that may exceed the allowed message sizes or that use too much bandwidth.

3.4. Regulatory considerations

It is important to consider the diversity of the applicable jurisdictions at sea when designing the PKI solution. This calls for a solution to be developed in a way that is acceptable for the International Maritime Organization (IMO) and all its member states.

Ships in international trade will have to relate to various international legal frameworks, mainly IMO instruments and the United Nations Convention on the Law of the Sea (UNCLOS) [3]. The latter is of limited relevance in this context except that it will regulate the jurisdiction of relevant regulations and laws that apply to the ship. In practical terms this will be the flag state for most operations on board, port/coast state law when ports are called on and IMO instruments for various regulations applicable for ships on international voyages or for innocent passage through other states' territorial waters.

Flag state law will vary but will generally reflect IMO requirements to safety and security on board the ship. This includes requirements for authentication, e.g. signatures and/or seals on ship certificates, proper signatures on logbook entries, etc. IMO has also published guidelines for use of electronic versions of ship certificates [4]. IMO instruments include provisions for mandatory ship reporting,
e.g. related to ship reporting areas and similar. Today, these requirements do not include any provisions for authentication of sender. However, national legislation, e.g. in Norway [5], can require or recommend that electronic reporting is used which in some cases also may include some form of authentication.

When calling at a specific port, the ship will also be required to follow national legislation related to mandatory reporting before or during the port call. This may or may not include provisions for electronic reporting and possibly requirements for authentication. In Norway, as an example, ships should use the Norwegian *SafeSeaNet single window* where authentication is implicit through a user code and a password. One should also keep in mind that some reports to the port and port services may result in various fees being payable. Errors or omissions in these reports can have direct economic consequences. Finally, one may need to consider export restrictions on certain types of advanced technology, which may make it impossible to fit corresponding technology to certain ships.

It would be very helpful if an international convention, e.g. an amendment to the FAL convention [2], would ensure the international acceptance of the electronic signatures enabled by an internationally managed PKI.

4. Related Work

There are some PKI systems already in operation in the maritime sector. This section presents a brief overview of some of the already established solutions and of the most relevant ongoing initiatives.

4.1. Established solutions

The Long Range Identification and Tracking (LRIT) system [6] collects position reports from ships worldwide and make them available to coastal states that have a legal interest in ships approaching or passing their shores. A PKI is operated by IMO to secure the communication between the distributed LRIT data centres. This is based on public cryptography technology and is used over ordinary Internet connections. The LRIT PKI could in principle be the basis for a wider scoped international maritime PKI, but one may have to change the basic cryptography mechanisms to reduce signature sizes.

SafeSeaNet [7] is a system similar to LRIT, but operated by European Maritime Safety Agency

(EMSA) and covering much more detailed information about ship movements and port calls. The same comments apply to SafeSeaNet as to LRIT, it could be used as basis for an international maritime PKI.

The International Hydrographic Office (IHO) also operates a type of PKI [8] that is used to encrypt and verify the authenticity and integrity of electronic charts. This includes cyber security protection, restricting access to only those elements that a customer has been licenced for; and authentication, i.e. to provide assurance that the data has come from approved sources.

4.2. New initiatives

The Maritime Connectivity Platform (MCP) [9] is an initiative to provide a communication system for the maritime industry, including an identity registry, service registry and a messaging service. Included in the framework is also a PKI, which is intended to be for authentication of, for example, vessels. This is a system that could lend itself to be an international agreed PKI. However, the business model for operating the MCP is still not defined.

ISO/TC 8 *Ships and marine technology* has proposed that a PKI should be used by the issuing party to digitally sign ship certificates [10]. The electronic signatures can then be verified by an inspector by means of computer, tablet or smart phone. In their report [11], ISO proposes the use of X.509 certificates and elliptic curve cryptography for generating and validating the signatures. ISO also envisions the use of a central public key repository, operated by e.g. IMO.

There are various initiatives to provide an authentication service for VDES and the establishment of an international PKI operated, e.g. by IMO has already been suggested [12]. The problem here is limited message length and high overhead resulting from even relatively compact elliptic curve signatures. As an example, the longest Application Specific Messages (ASM) messages in VDES use three message slots and are about 1200 bits long. Thus, a 512-bit long signature would use almost half of the message length. However, VDES also supports longer messages over higher capacity VDE (VHF Data Exchange – several 100 kilobits per seconds) where signature sizes are less problematic.

5. Analysis of unwanted events and PKI benefits

In order to determine the benefit of a PKI in the maritime sector, a set of thirteen use cases undergoing digitalisation were analysed as part of a Norwegian research project on cyber security for merchant shipping (CySiMS) [13]. These use cases have been introduced by Frøystad et al.[14], and are summarized in Section 5.1. In Section 5.2, we show how security experts participating in this project assigned general cyber security threats to unwanted events for maritime communication. With the aid of maritime domain practitioners, these unwanted events were subsequently linked to consequences for the individual use cases as shown in Section 5.3. This whole approach follows the thinking of bow-tie modelling, wherealternativecauses andconsequencesof unwantedevents motives the useof proactiveand reactivebarriers. More details about howthis can be represented and visualised are given by Bernsmed et al. [15]. The final result of the analysis is presented in Section 5.4, showing how the security functionality provided by a PKI benefits the use cases.

The CySiMS project focused on conventional shipping, but it should be clear from the use cases that this problem is even more acute for automated and autonomous ships. Here, there is no operator onboard to do "sanity checks" on messages and the computers rely on being able to trust both content and sender of digital messages. In particular, use-cases 3, 5, 8, 9 and 12 are relevant for autonomous ships.

5.1. Use Cases for the maritime sector

1) **Ship certificates:** Ships are required to carry original versions of a number of safety certificates on
board (e.g., International Tonnage Certificate, Safety Management Certificate, and International Anti-fouling System Certificate). These documents must be provided for

inspection by port state control (PSC) and others, such as during vetting by charterers.

2) **Single Window:** Ships entering a foreign port must declare important information on the ship, cargo, and persons on board, normally in good time before they enter.
3) **Safety information:** Different public services can provide Maritime Safety Information (MSI) to vessels in a specified area. This is typically gale warnings, warnings on ships in distress, ongoing search and rescue operations, etc. This is a receive only operation where the ship navigator is responsible for keeping track of these messages and, if necessary, react to them to aid in search operations or to avoid various dangers to safe navigation.
4) **Mandatory Ship Reporting Systems:** Ships entering and leaving ship reporting areas or VTS controlled areas are normally required to report this to the VTS or other reporting authorities.
5) **Nautical Information:** Ships are required to keep critical electronic databases up to date. This includes electronic charts, lists of navigation signals, etc.
6) **Operational exchange:** Ships communicate with owner, manager, charterer, or agents for operational purposes. This includes voyage orders, periodic reports from the ship or performance reports, e.g. in conjunction with charter contracts.
7) **Logbook:** The deck logbook is one example of a logbook kept on board, which can be inspected by the Port State Control (PSC) and that may be used as evidence in case of accidents. An electronic logbook needs to be signed at the time when the log entry was made. It must be impossible to tamper with a recording and recording should as much as possible be automatic.
8) **Traffic organisation advice:** Some services provide advice to the ship to make passage safer or more efficient. The master has to decide if the advice is used and will in principle look at this as any other type of general navigational information. This type of information is commonly sent from Vessel Traffic Services (VTS).
9) **Traffic organisation instructions:** This case is similar to the one above, but here the instructions are stronger than advice. This can be used in port areas and issued from a port VTS. The master is still responsible for safe passage and may refuse to follow instructions if they are deemed unsafe, but not following the orders may have operational or economic penalties (e.g., increased port fee or increased waiting time for pilot or berth).
10) **Telemedicine:** Ships have access to land-based advice during medical emergencies, but this is usually restricted to voice communication. In the future it is foreseen that this may be in part digitalized where e.g., pictures or EKG-data can be transmitted directly to specialists.
11) **Search and rescue:** During search and rescue operations, nearby ships are often used to assist. This can be to searching for persons overboard or to directly assist a ship in distress. The maritime rescue coordination centre (MRCC) or on scene commander can issue detailed instructions, e.g. search patterns, to the ships.
12) **Remote control:** It is possible to, e.g. remotely control a tug from the bridge of the ship being assisted. This will give the pilot and captain better information about both ships responses and improve coordination as well as reduce chances of misunderstanding in voice communication. This function is still on research stage.
13) **VDE Bulletin Board:** When a vessel enters the coverage area of a Terrestrial VDES base station it will receive the Terrestrial Bulletin Board (TBB) message. The TBB information includes important information on the use of VDE in the area. The TBB does not change often and should be transmitted in regular intervals.

5.2. Threats leading to unwanted events

In Table 1 we have enlisted threats towards the communication links between ship-ship and ship-shore. Note that threats related to physical access to ship systems or shore assets, as discussed by e.g. Rødseth et al. [16] and Jones et al. [17], are out of scope in this context.

Table 1: Communication related threats and unwanted events

General threat	**Unwanted event**
T1: Jamming of terrestrial link	E1: Loss of one or more messages
T2: Jamming of satellite link	E1: Loss of one or more messages
T3: Short DoS attack towards shore-based system	E2: Limited or no communication capacity for a short period of time (1-2 hours)
T4: Long DoS attack towards shore-based system	E3: Limited or no communication capacity for a long period of time (1-2 days, or more)
T5: Wiretapping of terrestrial link	E4: Confidential data overheard by an unauthorized actor
T6: Wiretapping of satellite link	E4: Confidential data overheard by an unauthorized actor
T7: Repudiation of transmitted message	E5: Data is received, but the sender denies having sent the data
T8: Repudiation of received message	E6: Data is sent, but the receiver denies having received the data
T9: Broadcasting of false messages on an open channel	E7: False data received by one or more actors listening to the broadcast channel
T10: Transmission of an unauthenticated message to a single actor	E8: False data received by the ship or the shore
T11: Retransmission of a previously trans-mitted message	E8: False data received by the ship or the shore

5.3. Consequences of unwanted events

As shown in Table 2, a single unwanted event can have consequences for numerous use cases.

Table 2: Consequences of unwanted events

Unwanted event	**Use case consequences**
E1: Loss of one or more messages	UC1-2, UC4, UC6-7: Possible delays, ship not seaworthy, ship arrest UC3, UC5, UC8-9, UC12: Possible collisions, grounding, damages to facilities UC10-11: Damages to health or loss of life UC13: VDES not available
E2: Limited or no communication capacity for a short period of time (1-2 hours)	Same as above
E3: Limited or no communication capacity for a long period of time (1-2 days, or more)	Same as above
E4: Confidential data overheard by an unauthorized actor	UC2: Leakage of business sensitive information, data privacy breach, loss of reputation UC6: Leakage of business sensitive information UC10: Leakage of sensitive health information
E5: Data is received, but the sender denies having sent the data	UC2, UC4: Possible delays, breach of contracts, lawsuits
E6: Data is sent, but the receiver denies having received the data	Same as above
E7: False data received by one or more actors listening to the broadcast channel	UC13: Spoofing of VDES services, possible collisions, blocking of harbours

Unwanted event	**Use case consequences**
E8: False data received by the ship or the shore	UC1-2, UC6: Fraud, smuggling of illegal goods, delays UC3, UC5, UC8-9, UC12-13: Possible collisions, grounding, damages to facilities UC4, UC7: Fines UC10-11: False alerts, damages to health or loss of life

A user survey was conducted to assess the criticality of the different consequences. In the survey, which was conducted on the premise that the ship had ordinary manning, the commercial consequences were generally considered the most severe, i.e. the possibility for detention in port, fines or the consequences of leaked sensitive information. This is probably because with a conventionally manned bridge, it is less likely that fraudulent message or jamming will cause major events as the crew directly or indirectly will verify the saneness of the received information.

However, with more automation onboard, and in particular with fully unmanned ships, the risk for major events may be significantly higher. The automation systems will be relied on more and the probability that false information can lead to unwanted events increases. This should also be seen in conjunction with increasing probability for "cyber terrorism", where enemy parties may want to disrupt international trade by, e.g. blocking an entrance to one of the world's large ports.

The exact nature and scale of the consequence will depend on properties of the ship (e.g. type of ship, size, and cargo) and the context it is operating in (e.g. at shore, in a busy area, geopolitical surroundings, weather conditions).

5.4. Security barriers provided by a PKI

In Table 3, the use cases are mapped to the security functionality that a PKI can offer. The mapping is derived from an analysis of the use case characteristics and their associated cyber security risks.

A special note regarding use case 1 and 7 should be made, since these are related to documents where the PKI is used to sign and verify documents stored on-board the ship and not during the actual communication. Signatures can ensure the integrity and the authenticity of the ship, crew member role and person signing the logbook entries or issuing party of a certificate. These documents are then self- protected, which enables them to be transferred over insecure as well as secure communication channels. However, with events 1-3 the content is lost or unavailable, which means that content protection has no real effect. Instead, a physical inspection of the documents might be needed, causing potential delays and extra costs.

The rest of the use-cases will require secure communication, as indicated by tick-marks in the columns AUT, INT, CON. This is short for authentication, integrity checks and confidentially respectively. E-DOC Sign is indicated where an electronic document kept on board needs a signature.

Use cases 3, 8-9, 11 and 13 share common benefits from message authenticity, availability, and integrity. This is because they typically involve information sent from shore to the ship, and the ship needs to be sure that this information can be trusted. A PKI can ensure the integrity of the message and the authenticity of the sender. Use case 5 is a special case that would also benefit from confidentiality since nautical information is typically bought from a nautical service provider and not classified as *open* or *free* data. Use cases 2, 4, 6 and 10 share similar benefits from a PKI allowing parties on ship or shore to authenticate themselves, to sign the data to be sent and to verify the identity of the recipient. Additionally, a PKI can ensure confidentiality when sending restricted information from ship to shore by either encrypting the data or communication channel. Use case 12 is our only ship-to-ship use case with requirements for a tamper proof communication link. This use case represents a wider range of services where ships need to trust each other, even when they encounter each other at open sea with only local radio communication available. For both this use case and use case 10, it might be more relevant to use the PKI to establish a longer-lasting secure

communication session rather than securing individual messages.

Table 3. Mapping of high-level use cases to relevant security functionality offered by a PKI. Actors marked * must be authenticated and arrows indicate the direction of the information flow.

Use Case	Identification and authentication	Secure communication			E-DOC Sign	Media	Unicast / Multicast
		AUT	INT	CON			
UC1 Ship certificates	Flag state auth.* → Ship → PSC					offline	N/A
UC2 Single Window	Ship* ↔ Port state authorities*					SatCom	U
UC3 Safety information	MSI provider* → Ship					VDES/ SatCom	M
UC4 Reporting	Ship* ↔ VTS*					VDES	U
UC5 Nautical information	Nautical Service* → Ship					SatCom/ VDES	U
UC6 Op. exchange	Ship operator* ↔ Ship*					SatCom	U
UC7 Log-book	Crew*→ PSC, Auth.					offline	N/A
UC8 TO Advice	Ship* ↔ VTS*					VDES	U
UC9 TO instructions	Ship* ↔ VTS*					VDES	U
UC10 Telemedicine	Ship* ↔ Medical Aid Provider*					SatCom	U
UC11 Search and rescue	Ship* ↔ MRCC*, SAR*					VDES	M
UC12 Remote control	Ship* ↔ Remote Ship*					VDES	U
UC13 VDE TBB	Bulletin Board* → Ship					VDES	M

In addition to required security functionality, Table 3 also outlines which communication channels the use cases will utilize. We can summarize that the PKI solution must be able to support authentication of a wide variety of communicating entities, which can be generalized as being either *Ships*, *Services*, *Organisations*, or *Individuals*. Ships and Services will need to communicate both over VDES and more general communication channels. Organisations and Individuals will primarily use their keys for offline digital signatures of electronic documents.

6. Conclusion

An internationally accepted and widely deployed PKI system will solve many of the security and trust challenges associated with the sharing of digital information in the maritime sector. In this paper we have outlined a number of relevant use cases and showed how a PKI system can provide security barriers to mitigate threats and consequences.

We have also pointed out the most relevant use cases for autonomous ships, which are related to automated processing and decision making based on message information, i.e. use cases 3, 5, 8, 9 and 12. In these cases the importance of source authentication and message integrity is very high.

A PKI needs to be designed with the specific maritime business constrains in mind; the most

important being the international nature of shipping, the lack of connectivity for ships that are far from shore, the network constraints associated with existing communication technologies and regulatory considerations.

Acknowledgments
The work presented in this text has been partially funded by the Norwegian Research Council project "CySiMS Service Evolution" under contract number 295969. It has also received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 815012 (AUTOSHIP).

References

[1] Lázaro, F., Raulefs, R., Wang, W., Clazzer, F. and Plass, S., 2019. VHF Data Exchange System (VDES): an enabling technology for maritime communications. *CEAS Space Journal*, *11*(1), pp.55-63.
[2] *Convention on Facilitation of International Maritime Traffic* (FAL Convention), Adoption: 9 April 1965; Entry into force: 5 March 1967, as amended.
[3] UNCLOS *United Nations Convention on the Law of the Sea*, Retrieved June 2020 from http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
[4] IMO, 2016, FAL.5/Circ.39/Rev.2, 20 April 2016, *Guidelines for the Use of Electronic Certificates*.
[5] Department of transport, Norway, *Forskrift om fartøys meldeplikter etter havne- og farvannsloven*, 2015, retrieved June 2020 fr om https://lovdata.no/dokument/SF/forskrift/2015-12-21-1790 (In Norwegian).
[6] IMO, 2020, MSC.1/Circ.1294/Rev.6, 8 April 2020 *Long-Range Identification and Tracking System, Technical Documentation (Part I and II)*.
[7] European Maritime Safety Agency (EMSA), *SafeSeaNet main page*, Retrieved June 2020 from http://www.emsa.europa.eu/ssn-main.html
[8] IHO, 2015, *IHO Data Protection Scheme* Edition 1.2.0, January 2015, IHO Publication S-63, International Hydrographic Bureau, Monaco.
[9] MCP consortium, 2020, *Maritime Connectivity Platform (MCP)*, Retrieved June 2020 from https://maritimeconnectivity.net/
[10] IMO 2017, FAL.2/Circ.131, 19 July 2017, *Requirements for Access to, or Electronic Versions of, Certificates and Documents, Including Record Books Required to be Carried on Ships*.
[11] ISO 2015, FAL 40/6/2, 31 December 2015, *Future Proof and Cost-Effective Standardization of Electronic Ship Certificates*, Input document to IMO FAL Committee.
[12] IALA, 2019, Guideline G1139, *The Technical Specification of VDES*, Edition 3.0, June 2019.
[13] The *Cyber Security in Merchant Shipping* (CySiMS) project, retrieved June 2020 from: http://cysims.no/
[14] Frøystad C., Bernsmed K., and Meland P. H., 2017, Protecting future maritime communication, *Proceedings of the 12th International Conference on Availability, Reliability and Security* (ACM) p 97.
[15] Bernsmed K., Frøystad C., Meland P. H., Nesheim D. A. and Rødseth Ø. J., 2017, Visualizing cyber security risks with bow-tie diagrams, *International Workshop on Graphical Models for Security* (Springer) pp 38–56.
[16] Rødseth Ø. J. and Lee K., 2015, Secure communication for e-navigation and remote control of unmanned ships, *Proc. of the 14th Conference on Computer and IT Applications in the Maritime Industries-COMPIT* vol 15.
[17] Jones K. D., Tam K., and Papadaki M., 2016, Threats and impacts in maritime cyber security, *IET Engineering & Technology Reference*, 2016.