Protecting Future Maritime Communication

Christian Frøystad
SINTEF Digital
Strindvegen 4
Trondheim, Norway 7034
christian.froystad@sintef.no

Karin Bernsmed
SINTEF Digital
Strindvegen 4
Trondheim, Norway 7034
karin.bernsmed@sintef.no

Per Håkon Meland*
SINTEF Digital
Strindvegen 4
Trondheim, Norway 7034
per.h.meland@sintef.no
per.hakon.meland@ntnu.no

ABSTRACT

Our oceans are filled with ships that take care of the most important distribution of goods in the world economy. Evolving from isolated chunks of hollow metal containers, ships are becoming more and more like interconnected floating computers, and thus increasingly exposed to unwanted cyber events. This paper shows how a Public Key Infrastructure (PKI) design can be applied to protect digital communication in the maritime sector. This includes new services depending on ship-to-ship, ship-to-shore and shore-to-ship datalinks, and where intentional and unintentional cyber threats can have severe consequences to the cargo, crew, ships and the environment. The design considers domain specific characteristics, such that bandwidth is limited and ships may be offline for long periods of time. In addition, international applicability and a cost-efficiency have been important drivers. We present design goals derived from workshops and surveys involving stakeholders from the maritime domain, outline the design of the proposed PKI and explain how it can be operated in global maritime setting.

CCS CONCEPTS

• **Security and privacy → Domain-specific security and privacy architectures**;

KEYWORDS

cyber security, maritime communication, PKI, VDES

ACM Reference format:
Christian Frøystad, Karin Bernsmed, and Per Håkon Meland. 2017. Protecting Future Maritime Communication. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017,* 10 pages.
https://doi.org/10.1145/3098954.3103169

1 INTRODUCTION

Maritime communication is currently undergoing major changes. The transition from analogue voice over Very High Frequency (VHF) radio to digital messages over VHF Data Exchange System (VDES) [14], and the introduction of satellite communication as an additional channel, means that the stress on the current communication links are reduced and new services can be introduced. Examples of envisioned future maritime communication scenarios include advanced e-Navigation, electronic reporting from ships to shore stations and ports, and remote control of tug boats and other types of unmanned ships [17]. Digital technology for ships is in continuous development, and the importance of cyber security to ensure safe and reliable operations is increasing. However, the awareness of cyber security in the maritime community is currently very low [6]. At the same time, it is well know that existing navigational systems are vulnerable to attacks [8, 19, 22], port systems have already been hacked for profit [3] and shipping is by some expected to become the "next playground for hackers" [23]. Attacks will typically be motived by profit, as a single container ship can carry more than 13000 containers, reaching a total value of $300 million [15]. Launching attacks making such a ship "not seaworthy", drifting into others or blocking busy ports can easily be a lucrative business for cyber extortionists.

Traditional cyber security on shore apply a host of well-known controls to avoid data compromise by hostile attackers or ignorant users. These are typically physical protection, encryption, electronic signatures, virus protection, firewalls, backups, intrusion detection systems and so on. Many of these controls are also applicable to ships, but shipping faces four particular and serious problems: 1) Ships are for extended periods self-reliant "villages at sea". The crew must manage the security of the data systems on the ship without support from specialists. 2) The complexity of the ship data systems is relatively high with many infotainment, administrative, safety and technical networks with different types of interconnections. 3) Ships are increasingly reliant on exchange of information between ship and shore, and this opens up new attack vectors targeting conventional data exchanges, as well as special purpose data exchange systems used only by ships. 4) Shipping is a low cost business. At the same time, existing data communication links are both expensive and has very limited bandwidth.

VDES is currently being standardised and is expected to be fully operational in 2021. The purpose of the work presented in this paper is to facilitate the adoption of the VDES technology, by proposing a solution for securing the services that will utilize this communication link. The research question pursued in this paper is how a Public Key Infrastructure (PKI) can be designed and operated for this purpose in an international maritime environment.

The paper is organised as follows. Section 2 gives an overview over state-of-the-art of maritime cyber security. Section 3 provides an overview of future maritime communication scenarios, explains

*Also with Norwegian University of Science and Technology.

ARES '17, August 29-September 01, 2017, Reggio Calabria, Italy

ACM ISBN 978-1-4503-5257-4/17/08…$15.00
https://doi.org/10.1145/3098954.3103169

our methodological approach and derives design goals for the security solution. In Section 4 we outline the design of the PKI, and in Section 5 we explain the operational processes, which include how to handle enrolment of entities and certificate expiration, renewal and revocation. Finally, Section 6 concludes the paper and points to future work.

2 STATE OF THE ART

As pointed out by ENISA [6], the awareness of cyber security in the maritime sector is low, and the overall sector lacks the capability to consistently assess and deal with cyber security threats. So far, the research community has mostly focused on vulnerabilities and weaknesses in existing ship navigational equipment, tracking and monitoring systems [1, 8, 19, 22]; very little has been done on designing security solutions for future maritime services. One notable exception is the "Maritime Cloud" platform[1] implemented by the Danish Maritime Authority (DMA), which is a proof-of-concept that demonstrates how identity management can be implemented in the maritime community. Even though this solution includes a PKI, they do not explain how the PKI will be operated once the certificates have been issued.

A recent working document from an IALA committee [18] recognises the need to increase the security of information transferred over VDES and outlines a method for public key distribution for authenticating the source of ship-to-shore and ship-to-ship application data. Further, they propose that public keys can be distributed over any standard maritime communication means, including VDES. The committee points out that more work is needed to decide how the PKI infrastructure should be set up and operated. The ISO/TC 8 Ships and marine technology committte[2] has investigated how digitally signed ship certificates can be standardized in the maritime domain, and propose to use a PKI to implement this [13]. Even though their work focus on protecting electronic documents rather than securing message communication, it shows that the International Organization for Standardization (ISO) is ready to support standardization of a digital signature solution, which includes setting up an international PKI.

3 SECURING FUTURE MARITIME COMMUNICATION

Figure 1 provides an overview over the future maritime communication ecosystem. The figure illustrates a diverse set of interactions, including information exchanges between ships, between ships and organisations, for example ports, Vessel Traffic Services (VTS) and Shipping Coordination Centres (SCC), and between ships and services, for example e-Navigation and Medical Aid Providers (MAP). Which communication channel to use for which service will depend on the ship's location (at port, near shore or at sea), with whom it is communicating and what type of information that is to be transmitted.

Our approach for deriving design goals has been to study the maritime communication literature, standards and reports to define a set of future maritime communication use cases described in [16]. Starting in 2016, we also arranged a series of workshops together

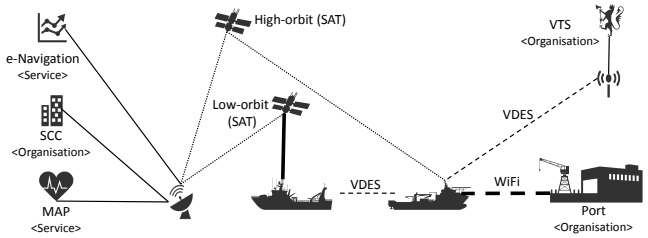

Figure 1: High-level overview over the future maritime communication ecosystem.

with various stakeholders from suppliers, service providers, coastal authorities, security professionals and domain experts, where we further developed descriptions on how such use cases are envisioned to be implemented in the near future. The use cases can be summarized as:

- *UC1 Ship certificates*, which describes the management of electronic ship certificates. The use case outlines how such certificates can be issued, verified by third parties in foreign ports, on-board inspection and validation of the certificates, and how the ship certificates can be renewed and/or revoked.
- *UC2 Single Window*, which outlines the use of the Maritime Single Window for declaring data on the ship, cargo and persons on board before the ship enters a foreign port.
- *UC3 Safety information*, which describes the transmission of Maritime Safety Information, e.g., gale warnings and ongoing search and rescue operations to ships in a specific area.
- *UC4 Reporting*, which covers the mandatory reporting that ships must perform when entering or leaving a VTS controlled area.
- *UC5 Nautical Information*, which includes updating the nautical documents, including charts, required for the ship's intended voyage.
- *UC6 Operational exchange*, which describes how ships communicate with owner, manager, charterer or agents for operational purpose.
- *UC7 Log book*, which covers electronic logs book kept on board.
- *UC8 Traffic organisation advice and UC9 Traffic organization instructions*, which refers to the messages exchanged between the ships and a VTS.
- *UC10 Telemedicine*, which covers remote communication between ships and medical aid providers at land.
- *UC11 Search and rescue (SAR)*, which includes the exchange of instructions and status messages to coordinate a SAR operation.
- *UC12 Remote control*, which describes remotely controlling a tug from the bridge of the ship being assisted.
- *UC13 VDE Bulletin Board*, which broadcasts data on how the VDES communication link is to be used in a certain area.

An additional workshop was used to analyse the security needs of these use cases based on what needed to be protected (primary and secondary assets) and which cyber incidents could have consequences to these assets. Specifically, we had one group of people working on how services could be attacked, and another group working on how they should be protected. The *protection group* had to constantly disclose what their protection mechanisms were, while the *attacking group* only revealed their methods in the end. We did

[1] http://developers.maritimecloud.net/identity/index.html
[2] https://www.iso.org/committee/45776.html

this experiment to encourage competition among the participants and follow the principle that security can not be a hidden feature.

This workshop was followed by an online survey among additional stakeholders to gather supplementary information about security concerns related to the use cases. The detailed results of this risk assessment has been described in [16]. A final workshop was arranged in February 2017 to present and evaluate the design goals and proposed solution that we describe in the following sections.

3.1 Needed security services

In Table 1, the use cases are mapped to required security functionality.

All use cases require the actor(s) transferring the information to identify and authenticate itself (themselves). Two of the uses cases (UC1 and UC7) focus on the generation, verification and revocation of digital signature on electronic documents, such as ship certificates and log books. The rest of the uses cases will require secure communication, where integrity and authenticity of the transmitted messages stand out as the most important security functionalities. Confidentiality protection will also be important in some scenarios, in particular for transmission of commercially valuable data, such as nautical charts (UC5), voyage reports (UC6) and privacy sensitive data, such as passenger and crew lists (UC2, UC4) and medical information (UC10).

From Table 1 we can conclude 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" (VTS' and nautical services), "organisations" (flag and port state authorities, ship owners, medical aid providers and maritime safety information (MSI) providers)), or "individuals" (crew). Ships and services will need to communicate both over VDES and more general communication channels[3]. Organisations and individuals will primarily use their keys for offline digital signatures of electronic documents. The table also outlines the need for authenticity, integrity and confidentiality protection of messages transferred over SAT (and other higher capacity communication channels) between the ships and the port state authorities, ship owners and service providers (UC2, UC6, UC10). Note that, in contrast to the other use cases, which describe short message transmissions, UC10 (Telemedicine) may require that a secure synchronous session is established between the communicating actors.

3.2 Constraints

In addition to the required security functionality, a number of constraints associated with the maritime communication will affect the design of the PKI solution.

First, the solution has to be adapted to the large number of actors involved. At the time of writing, the International Maritime Organization (IMO) [11] has 171 member states (flag states and port states) and there are approximately 110 000 registered ports. There are between 100 000 and 150 000 ships that are operating internationally today and each ship usually have 10-30 crew members who are authorized to operate critical systems on board. Second, cost will be an important constraint. Shipping is a low cost business and this imposes limitations on which solutions could be acceptable to the industry. The costs associated with implementing and operating the PKI must therefore be kept sufficiently low for all the intended users, such as ship owners, port state authorities and ports, flag states and their recognized organisations as well as the operators of any security mechanisms included in the solution. Third, the communication capacities of the different networks needs to be taken into account. Referring to the ecosystem outlined in Figure 1, VDES is expected to become the bottleneck with an expected shared capacity of 153.6 kbps [14]. VDES will be available to ships that are near shore and between nearby ships. The satellite communication link (SAT) will offer between 100 kbps – 8 Mbps, but will, in contrast to VDES that is free of use, be expensive to utilize. WiMAX and WiFI are in most cases free of charge but are only available to ships that are at port. It is therefore important to include both the stress on communication links and the cost of using these links when designing the PKI solution.

[3]This includes SAT, general SATCOM, WIFI at ports, LTE, 3G, 4G and 5G near shore.

3.3 Design goals

Based on the envisioned use cases, their security needs and the applicable constrains, we have derived the following 10 design goals:

(1) The PKI solution must support authenticity, integrity and confidentiality protection of information exchanged between a wide variety of users, including (but not limited to) ships, organisations, services and individuals.
(2) The PKI solution should be independent of the communication link in use (VDES, SAT, WiFi, etc.).
(3) The ship component of the PKI solution should be retrofittable to existing bridge systems and must be easy to operate for on-board crew without any specific technical knowledge.
(4) The cryptographic properties of the PKI solution must be verifiable also when ships are offline.
(5) The PKI solution must be adapted to the maritime communication infrastructure where bandwidth is limited.
(6) The costs of the PKI solution should be minimized.
(7) The deployment and operation of the PKI infrastructure, including enrolment, distribution and revocation of PKI certificates, must be manageable in a global environment.
(8) The PKI solution must be acceptable by the international maritime community and fit with the existing roles, responsibilities and trust relationships of its key stakeholders (IMO, flag states, coastal states and ship owners).
(9) The PKI solution must be compliant with applicable maritime legislation, regulation and standards worldwide.
(10) The PKI solution should enable migration to future cryptographic solutions without excessive costs or efforts.

4 THE DESIGN OF THE PKI SOLUTION

This section outlines the design of the Public Key Infrastructure (PKI) that we propose. The PKI is based on X.509 [4], which is the most established standard for managing public keys and which is commonly used for deploying certificate-based architectures on the Internet.

Table 1: Mapping of high-level use cases to relevant security functionality. The use cases that utilize VDES are shaded with light gray colour. Actors marked ∗ must be authenticated; arrows indicate the direction of the information flow

Use Case	Identification and authentication	Secure communication			Electronic document signature	Media	Unicast/ Multicast
		Message authenticity	Message integrity	Message confidentiality			
UC1 Ship certificates	Flag state auth.* → Port state auth.				✓	offline	N/A
UC2 Single Window	Ship* ↔ Port state auth.*	✓	✓	✓		SAT	U
UC3 Safety information	VTS*, MSI provider* → Ship	✓	✓			VDES, SAT	M
UC4 Reporting	Ship* ↔ VTS*	✓	✓	✓		VDES	U
UC5 Nautical information	Ship* ↔ Nautical Service*	✓	✓	✓		VDES, SAT	U
UC6 Operational exchange	Ship owner operation* ↔ Ship*	✓	✓	✓		SAT	U
UC7 Log book	Crew*				✓	offline	N/A
UC8 Traffic org. advise	Ship* ↔ VTS*	✓	✓			VDES	U
UC9 Traffic org. instructions	Ship* ↔ VTS*	✓	✓			VDES	U
UC10 Telemedicine	Ship* ↔ Medical Aid Provider*	✓	✓	✓		SAT	U
UC11 Search and rescue	Ship* ↔ VTS*	✓	✓			VDES	M
UC12 Remote control	Ship* ↔ Remote Ship*	✓	✓			VDES	U
UC13 VDE Bulletin Board	Bulletin Board* → Ship	✓	✓			VDES	M

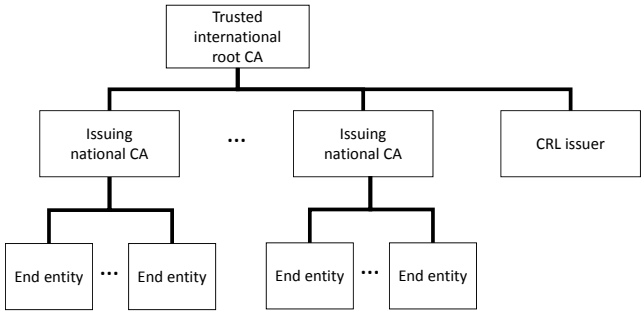

Figure 2: The general model of the PKI trust hierarchy.

4.1 The PKI trust hierarchy

The general model for the PKI trust hierarchy that we propose is illustrated in Figure 4. There are three layers in this model:

- Trusted international root Certificate Authority (CA), which should serve as the root of trust in the PKI hierarchy
- A number of Issuing national CAs, which should administrate X.509 certificates on a national level.
- End entities, which are ships, services, organizations and individuals that need to communicate securely.

In addition, an entity called "CRL issuer", responsible for issuing Certificate Revocation Lists (CRLs), will be needed.

The trusted international root CA should be operated by an internationally recognized organisation with impact in the maritime domain, and which has the capability of operating and maintaining a X.509 certificate authority (including a Certificate Server and a Certificate Signing Request (CSR) server) that can be available 24/7 from anywhere in the world[4].

The Issuing National CAs should, as the name indicates, be operated by organizations on a national level. The envisioned candidates for this role are the Flag State administrations associated with each country.

4.2 Components included in the PKI solution

An overview over the components necessary for operating the proposed PKI solution is illustrated in Figure 3. These are:

- An air gapped Root CA server[5], which uses a CSR submission server to fetch and sign X.509 Certificate Signing Requests (CSRs) from the Issuing national CAs.
- A number of Issuing national CA servers, which fetch and sign Certificate Signing Requests (CSRs) from their associated end entities.
- A Certificate server, which serves as a publicly available repository for all the signed X.509 certificates and certificate revocation lists (CRLs).
- A CRL submission server, which unifies the Certificate Revocation Lists (CRLs) from the Root CA and the Issuing National CAs and publish them on the Certificate server.
- End entities, which share certificates with each other in order to establish secure communication.
- PKI Units, which should be installed on-board the ships.
- Smartcards and Hardware Security Modules (HSMs), which are used to store the private key(s) and the root CA certificates at the end entities. The smartcards should be physically embedded in the PKI Units.

[4]IMO [11] is a candidate that fulfil these requirements. IMO is already operating the root CA for the LRIT system [7] and has also been proposed by ISO to act as the root of trust in a PKI for digital signatures of ship certificates [13]. Other potential candidates for operating the root CA are IALA [9], EMSA [5] or IHO [10].

[5]The Root CA represents the root of trust in the PKI system and if this component is compromised the whole PKI will be compromised. For security reasons we therefore recommend that the Root CA server is realised as an "air gapped" (i.e. offline) workstation/PC installed in a secure and trusted environment.

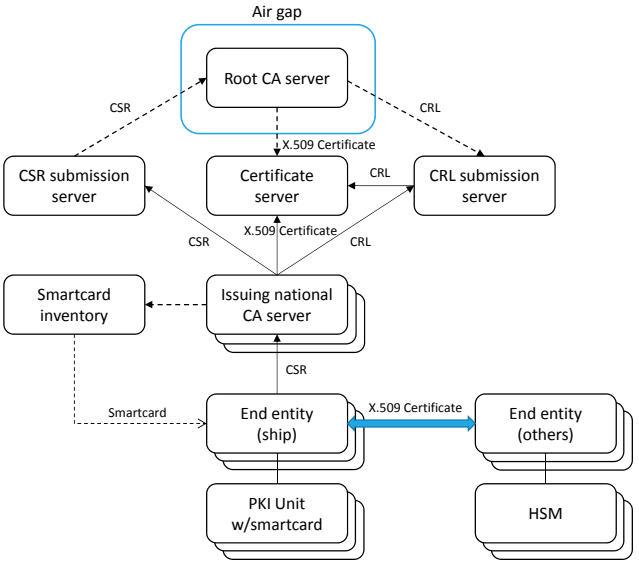

Figure 3: The main components included in the PKI.

- A Smartcard inventory, which keeps track of who possesses and owns each smartcard in the supply line and the end entities.

In Figure 3, dashed lines are used for logical (offline) connections and fixed lines are used for (online) network connections. The thick bidirectional arrow illustrates the use of the X.509 certificates to secure the connection between end entities. The interactions between these components will be further described in the next section (Operational processes).

As illustrated in Figure 3, each ship should have a PKI Unit with a smartcard to carry its security credentials. This unit should be classified as navigational equipment, which means it needs to have an expected lifetime of 10 years. Figure 4 shows a the PKI Unit design, with separate subsystems for general and bridge network usage. This way the X.509 certificates and the smartcard can be made available to the services and applications that need it, across the boundary of the bridge network on board the ship. The X.509 certificate cache holds all the national issuing CAs as well as the official CRL, delta CRLs and any other X.509 certificates the ship would need to store. Each subsystem has a request handler, which receives requests for digital signatures, or validations/verifications of such signatures, fetches the correct X.509 certificate and asks the smartcard to perform any cryptographic operations. The subsystem connected to the general network has a X.509 certificate updater, which is responsible for updating the X.509 certificate store at designated hours. Only the certificate updater shall be allowed to write data to the certificate cache, the request handlers shall only be allowed to fetch data.

The root CA certificate and the ship's private keys are stored on the smartcard, while all certificates fetched from the certificate server are stored in the Certificate Cache. The relevant request handler is responsible for obtaining the required information, preparing and queuing cryptographic operations for the smartcard, which performs them using the inherent root CA certificate, the smartcard private key and certificates from the certificate cache.

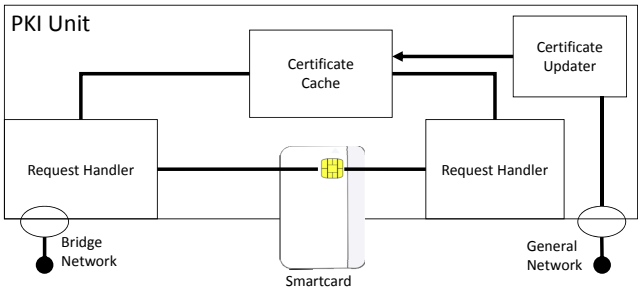

Figure 4: A logical design of a PKI Unit with separate subsystems for general and bridge network usage.

4.3 Key material and algorithms

An important consideration when designing a PKI solution is what length of keys to use for how long time. The stronger the keys, the longer they can be assumed to be secure, but strong keys will cause a larger overhead on the network and require more processing power. We had to conduct a study on suitable key material and algorithms for the maritime PKI solution, which lead us to propose key lengths and algorithms for the root CA certificate, the issuing national CA certificates and the end entity certificates as indicated in Table 2.

A fundamental design principle of cryptography is to never use the same key pair for signing and encryption [2]. Moreover, key pairs used for authentication of entities will most likely need longer life-time than the keys used to protect a message conversation. The "Key Usage" extensions defined in Table 2 will therefore put usage restrictions on the key contained in the certificates.

Note that, due to the limited bandwidth and potentially high bit error rate of the radio link, it might be necessary to introduce certificates with shorter keys that can be used for ship-to-ship and ship-to-shore communication over VDES. However, this needs to be weighted carefully against the information to be protected. Since neither the VDES or the future maritime services are sufficiently specified at this time, we propose that the key length for certificates related to VDES shall be decided at a later time when the standard has matured. Some of the entries in Figure are therefore marked "To Be Decided" (TBD).

5 OPERATIONAL PROCESSES

This section outlines how the Public Key Infrastructure (PKI) described in the previous section will be operated, with a focus on the ship end entity because this is where most of the constrains apply.

The operational processes for the Public Key Infrastructure (PKI) described in the previous section are 1) Enrolment, in which an entity applies for and receives a signed X.509 certificate, 2) Loading, in which the X.509 certificates are distributed and loaded to the ships, 3) X.509 Certificate use, in which the entity uses a certificate for secure communication, 4) X.509 Certificate expiration and renewal, in which certificates run out of date and are renewed, and 5) Revocation, in which X.509 certificates that are not valid anymore are revoked from the trust hierarchy.

These processes will involve the following actors:

Table 2: An overview of the recommended key material and algorithms for the maritime PKI

Entity	Security service	Key Usage	Algorithm	Key Length	Lifetime
Ship	Authenticity and integrity protection	digitalSignature, nonRepudiation	ECDSA	256 bit	3 years
	Encryption	dataEncipherment	TBD	256 bit	3 years
	Secure session establishment	keyEncipherment, keyAgreement	TBD	256 bit	3 years
Ship - VDES	Authenticity and integrity protection	digitalSignature, nonRepudiation	ECDSA	TBD	TBD
	Encryption	dataEncipherment	TBD	TBD	TBD
	Secure session establishment	keyEncipherment, keyAgreement	TBD	TBD	TBD
Service	Authenticity and integrity protection	digitalSignature, nonRepudiation	ECDSA	256 bit	3 years
	Encryption	dataEncipherment	TBD	256 bit	3 years
	Secure session establishment	keyEncipherment, keyAgreement	TBD	256 bit	3 years
Service - VDES	Authenticity and integrity protection	digitalSignature, nonRepudiation	ECDSA	TBD	TBD
	Encryption	dataEncipherment	TBD	TBD	TBD
	Secure session establishment	keyEncipherment, nonRepudiation	TBD	TBD	TBD
Organisation	Electronic document signatures	digitalSignature, nonRepudiation	ECDSA	256 bit	3 years
	Secure session establishment	keyEncipherment, keyAgreement	TBD	256 bit	3 years
Individual	Electronic document signatures	digitalSignature, nonRepudiation	ECDSA	256 bit	3 years
Issuing national CA	PKI certification and revocation	keyCertSign, cRLSign	ECDSA	256 bit	10 years
Root CA	PKI certification and revocation	keyCertSign, cRLSign	ECDSA	384 bit	20 years

- *Root CA Operator*, which is the term used to describe the organisation in charge of maintaining and running the root of trust in the PKI.
- *Issuing CA Operator*, which is the term used to describe the organisation in charge of maintaining and running an Issuing national CAs.
- *Smartcard Issuer*, which is the term used to describe the manufacturer of the smartcards that are used to store the private keys and root CA certificates for the ships.
- *PKI Unit Supplier*, which is the term used to describe the manufacturer of the PKI unit that should be installed on board the ships.
- *PKI Sponsor*, which is the term used to describe the person, at any given organisation or company, responsible for interacting with the Issuing CA Operator.
- *Engineer*, which is the term used to describe the person, at any given shipping company, responsible for installing the PKI unit at a ship.

5.1 X.509 certificate enrolment

X.509 certificate enrolment includes the process of registration, where an entity makes itself known to the Certificate Authority (CA), initialization, which includes generating the key material (i.e. the private and the public key), and certification, where the CA issues a X.509 certificate for the entity's public key and returns the certificate to the entity.

5.1.1 Enrolment of the Root CA. To enrol the Root Certificate Authority, the Root CA Operator must physically access the Root CA server and create a new X.509 certificate. The process for creating a new Root CA certificates consists of three steps:

(1) Generate a key pair.
(2) Self-sign the public key with the private key.
(3) Export the CA certificate and make it publicly available.

The third step includes a secure out-of-bands transfer of the CA certificate to the Smartcard Issuer, so that it can be installed on the smartcards during the ship enrolment process, as well as publishing the CA certificate on the Certificate Server.

The validity period of the CA root certificate should be set to 20 years. Ten years is the expected lifetime of the VDES communication equipment on-board the ships and an expired root CA certificate should not be the reason why the PKI Unit needs to be replaced before the VDES equipment fails.

5.1.2 Enrolment of the issuing national CAs. To enrol an Issuing National CA, the Issuing CA Operator must physically access the issuing national CA server and create a Certificate Signing Request (CSR), which must be signed by the root CA. This process consists of the following steps:

(1) Generate a key pair
(2) Export the public key and make it available to the root CA through a secure out-of-band channel
(3) Export a Certificate Signing Request (CSR) and submit it to CSR submission server
(4) Download the signed X.509 certificate from the Certificate Server and make it publicly available

The third step includes two activities performed by the Root CA Operator: 1) verifying that the CSR matches the public key from step 2 and 2) publishing the X.509 certificate on the Certificate Server

The validity period of the issuing national CA certificate can be set to up to 10 years, but not beyond the validity of the root CA certificate.

5.1.3 Enrolment of the ships. Enrolment of ships into the PKI will require multiple steps and actors. Prior to the enrolment of the ships, the Smartcard Issuer must perform a number of initialization functions of the smartcards. This includes generating a set of private/public key pairs for all the smartcards. The public keys should

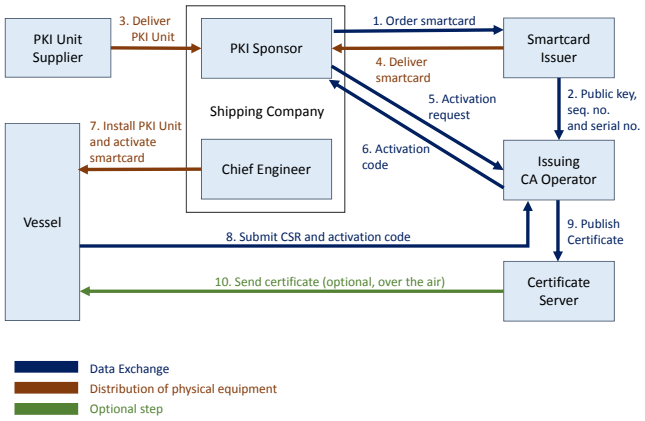

Figure 5: Enrolment of a ship into the PKI.

then be exported from the smartcards along with their sequence numbers and the serial numbers of the smartcards. This information must then be sent to the national Issuing CA Operator so that it will know which smartcards that are allowed to request X.509 certificates in the future. This reduces the risk that unauthorised ships are enrolled into the system.

Also, as a part of the initialisation, the Smartcard Issuer needs to pre-install the root CA certificate on all the smartcards.

The enrolment of a ship into the PKI consists of the following steps, which are illustrated in Figure 5:

- The PKI Sponsor orders a smartcard from the Smartcard Issuer (step1).
- The Smartcard Issuer initialize the smartcard (see above) and sends the public keys, together with the sequence numbers and serial number of the smartcard, to the Issuing CA Operator (step 2).
- The PKI Sponsor receives a PKI unit from the PKI Unit Supplier (step 3) and a smartcard from the Smartcard Issuer (step 4). The PKI Sponsor sends an activation request with relevant ship details to the Issuing CA Operator (step 5) that returns an activation code (step 6).
- The Engineer can now install the PKI Unit and activate the smartcard (step 7). The smartcard will then generate a Certificate Signing Request (CSR), which must be sent to the Issuing CA Operator together with the activation code (step 8).
- The Issuing CA must then verify the activation code, validate the CSR, sign the ship X.509 certificate and publish the signed certificate on the Certificate Server (step 9).
- As an optional step, the signed X.509 certificate can be sent back to the ship using any existing communication channel (step 10).

The enrolment process for the ships presented here has been designed to be as simple as possible for the shipping companies, while still being sufficiently secure. The solution will however, require some technical competence regarding PKI management in all the shipping companies.

The validity period of the ship X.509 certificates should be set to 3 years, but not beyond the validity of the issuing national CA certificate.

5.1.4 Enrolment of other entities. There are numerous options for enrolling other types of end entities, i.e. organisations, services and individuals into the PKI system, and it will be up to the individual Issuing National CA Operators to decide how such a process should be implemented.

Similar to the ship X.509 certificates, the validity period of certificates for other end entities should be set to 3 years, but not beyond the validity of the issuing national CA certificate.

5.2 Loading X.509 certificates onto ships

Once the end entities have been enrolled into the PKI system, they can start exchanging X.509 certificates to secure their communication. For end entities with permanent Internet connections, the common practice is to exchange certificates every time they initiate a communication. However, this approach will not work well for ships, which have a limited bandwidth when at sea.

We therefore propose that all relevant X.509 certificates are loaded into the certificate cache in the PKI Unit when the ship is in port. The first update of the cache will be in the order of 100s of megabytes, but subsequent updates will be in the order of 5-10s of megabytes.

Since a ship might be at sea for several weeks without calling a port, the ship might not carry all the latest X.509 certificates at all times. This aspect was discussed in one of the stakeholder workshops, which concluded that it is acceptable that both certificates and CRLs occasionally may run out of date. For the relatively few cases where a ship receives information from an entity for which it does not hold the relevant certificate, those entities can exchange certificates on the fly.

5.3 X.509 Certificate Use

Having access to the X.509 certificates of other entities, any enrolled entity can securely initiate operations requiring cryptographic protection. As explain in Section 3.3, the certificates can be used for:

- Message authenticity and integrity protection
- Message encryption
- Secure session establishment
- Electronic document signatures

This usage is based on traditional cryptographic functions and does not need further explanation in this paper. In addition to these four services, the Root CA and Intermediate National CA certificates should be used for certification and revocation. These have domain specific characteristics and are therefore given more attention in the following subsections.

5.4 X.509 Certificate Expiration and Renewal

Eventually, any certificate will expire, and to prevent connectivity issues, there must be mechanisms in place for graceful renewal of all the certificates.

5.4.1 Graceful renewal of X.509 certificates. To ensure a smooth transition, the following process should be followed. Every ten years, a new root CA certificate should be established[6] and run in

[6]The root CA can either renew its X.509 certificate with the same key pair that was used before, or the certificate can be renewed with a new key pair. The decision should

parallel with the existing one. During this transition period, the root CA must sign all Certificate Signing Requests (CSRs) from the Issuing National CAs with its new X.509 certificate. All new smartcards that are produced during this transition period must have the both the new and the old root CA certificate installed. After the ten-year transition period has passed, all Issuing National CAs and ships can be assumed to have migrated to use the new root CA certificate, and the old root CA certificate can hence be retired.

Similarly, three years before an Issuing National CA certificate expires, a new Issuing National CA certificate should be established and run in parallel with the existing one. During this transition period, the Issuing National CA must sign all Certificate Signing Requests (CSRs) from its associated end entities with its new X.509 certificate. After the three-year transition period has passed, all valid end entity certificates should have a signature from the new Issuing National CA certificate, and the old Issuing National CA certificate can hence be retired.

End entities should submit new CSRs when they enrol into the PKI system for the first time, when their existing X.509 certificates are about to expire, and if their existing certificates have been revoked.

The process is illustrated in Figure 6. The red lines illustrate how the Root CA signs Issuing National CA CSRs and the orange lines illustrate how Issuing National CAs sign end entity CSRs.

5.4.2 Ship rekeying. To avoid having to replace the smartcards on the ships when their X.509 certificates expires, rekeying should be used. Rekeying means replacing an existing key pair with a new key pair and issuing a new certificate. This process will be initiated either when the current ship certificate is about to expire or as a result of certificate revocation.

In due time (e.g., a few months) before the ship X.509 certificate expires, the PKI unit should increment the key pair on the smart card and initiate a new CSR. The new key pair should not be used before the new certificate has been fetched from the Certificate Server and installed on the smart card. To prevent connectivity issues, there should be some overlap (e.g., a few weeks) in the validity of the old and the new certificates.

When all key pairs have been used, the smart card should go to a state where it cannot be used anymore. It is the responsibility of the Issuing National CA Operator to keep track of when this is about to happen, as it knows all public keys for each smart card and their sequence. The Issuing National CA should therefore be used to plan for smart card replacement on the ships.

With this solution, the renewal of a ship X.509 certificate will be both simple and secure, since the ship enrolment process relies on pre-generated key pairs stored on the smartcard. The Issuing National CA Operator already knows all public keys that belong to a ship and the PKI Sponsor has already guaranteed that the current information is correct. Note that, as the root CA certificate is embedded on the ship smartcards, this means that a smartcard cannot be used after its root CA certificate has expired. It is not possible to update the root CA certificate, and consequently, new smartcards must be installed and enrolled for all the ships at least every 20th year[7].

be based on a number of factors, including the time that has passed since the original root CA certificate was generated, the length of the existing root CA private key and the risk that the root CA private key has been obtained by a malicious user.

5.5 X.509 Certificate Revocation

An X.509 certificate is generally valid until it expires. However, an issued certificate might need to be revoked for different reasons. Some might be revoked because the ships have been transferred to another owner, gained a new certificate, and thus the old certificate should no longer be valid. It might also be the case that a private key has been stolen, or lost, in which case any corresponding certificate would need to be revoked. This applies for issuing CAs and end entities alike. If the private key of the root CA is compromised, the entire PKI would need to be re-established from the ground up.

Due to the offline nature of the maritime domain, we cannot rely on modern web based revocation methods such as OCSP [21], but rather build a scheme on the more offline suitable Certificate Revocation List (CRL) [4]. In order to keep the network traffic to a minimum, long lived CRLs combined with frequent delta CRLs should be used. Furthermore, the evaluation workshop discussed the loading of CRLs and certificates, and concluded that it is sufficient that new CRLs are loaded when the ship is in port. Should the operator of the ship want more frequent updates, this can be done by satellite connection.

Figure 7 illustrates how X.509 certificate revocation can be handled in the maritime domain. As can be seen, a CRL issuer receives CRLs from the individual issuing national CAs and the trusted international root CA, unifies the content into one CRL, and offer this joint CRL to the end entities. While CRLs might become large, delta CRLs will be small. Thus, if every issuing national CA were to regularly send out (mostly empty) delta CRLs, a very large proportion of the traffic would be signatures, headers and formatting, rather than actual CRL data. Therefore, the unification of CRLs and delta CRLs are handled on shore, rather than having each end entity do the work. The CRL issuer is part of the certificate hierarchy on the same level as the issuing national CAs, as was illustrated in Figure 2.

The PKI solution should use long lived CRLs issued once a year from a central CRL issuer which unifies CRLs from all the issuing national CAs and the root CA. Additionally, delta CRLs should be issued once a week after the same model as the CRLs.

6 CONCLUSIONS AND FUTURE WORK

There is a clearly identified need for a PKI solution especially designed for the maritime domain. A variety of different users have to communicate securely in order to exchange critical information and ensure the safety of goods, passengers, crew and the environment. It is not cost-effective to implement, manage and maintain many parallel systems for similar purposes over different datalinks and geographical regions, and we argue that single 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 same

[7] An alternative to distributing new smartcards to all the ships is to implement an over-the-air distribution mechanism that installs new root CA certificates on the smartcard. However, this solution requires that the new root CA certificate is signed by the old root CA private key, which results in "chaining" of the certificates. We do not recommend this solution since it considered to be less secure.

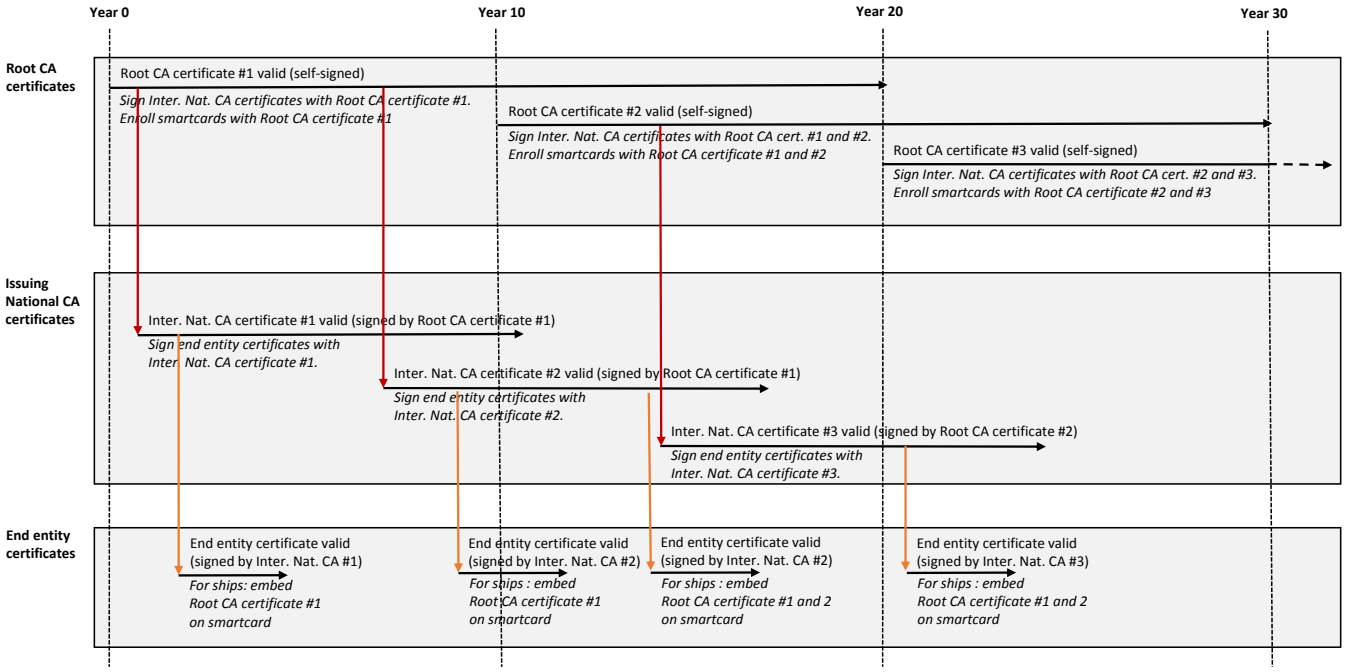

Figure 6: The X.509 certificate expiration and renewal process.

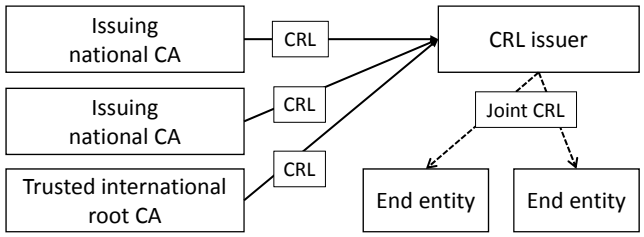

Figure 7: CRLs from multiple sources are collected and distributed through a CRL issuer.

solution can be used to generate and validate digital signatures of, for example, electronic ship certificates and logbooks, even when there are no communication links available during on-board inspections. To minimize the overhead when utilizing the emerging VDES technology, which will have a very limited network capacity, and for the solution to work for ships that are unable to contact the CA, the use of on-board local caches and accepting off-shore eventual consistency of certificates and CRLs will be needed.

The use of X.509 digital certificates to bind the cryptographic keys to participating entities is well-recognized and does not require substantial implementation effort, since there are many available software libraries for this. However, establishing an international trust hierarchy is something that will require more of an political effort rather than technical. For the PKI solution to be adopted by the worldwide maritime community, it needs to be standardized, and the results presented in this paper are being used as input to such an ongoing process.

It is also important to consider how and where private keys and root CA X.509 certificates should stored and processed on-board the ships themselves. There are several options on how this can be realized by the suppliers, but we recommend taking advantage of commercially available smartcards, that are already self-protected from tampering and have built-in strong cryptographic libraries. Similar approaches have been proven to be successful in related transportation domains such as for land-based vehicles (e.g. [20]) and aviation communication (e.g. [12]). Physical protection of the PKI Unit must always be present to avoid theft or sabotage, and schemes for physical maintenance, replacements and on-shore inventory management must be established at central ports around the world.

ACKNOWLEDGMENTS

The research leading to these results has been performed in the CySiMS project, which received funding from the The Research Council of Norwegian under Grant No.: 256508, and the SafeCOP-project, which received funding from the ECSEL Joint Undertaking under Grant No.: 692529.

REFERENCES

[1] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. 2014. A Security Evaluation of AIS Automated Identification System. In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14)*. ACM, New York, NY, USA, 436–445. https://doi.org/10.1145/2664243.2664257

[2] Elaine Barker. 2016. NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management. (2016). https://doi.org/10.6028/NIST.SP.800-57pt1r4

[3] BBC News. 2013. Police warning after drug traffickers' cyber-attack. (2013). http://www.bbc.com/news/world-europe-24539417

[4] D Cooper, S Santesson, S Farrell, S Boeyen, R Housley, and W Polk. 2008. RFC 5280-Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. (2008). https://www.ietf.org/rfc/rfc5280.txt

[5] EMSA. 2017. European Maritime Safety Agency. (2017). http://www.emsa.europa.eu/

[6] ENISA. 2011. *Analysis for Cyber Security Aspects in The Maritime Sector*. Technical Report November. 31 pages. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at

[7] European Maritime Safety Agency (EMSA). 2013. *Annex 3 LRIT International Data Exchange (IDE) Functions and Architecture*. Technical Report.

[8] Alan Grant, Paul Williams, Nick Ward, and Sally Baske. 2009. GPS Jamming and the Impact on Maritime Navigation. *Journal of Navigation* 62, 2 (2009).

[9] IALA. 2017. Assisting in safe navigation. (2017). http://www.iala-aism.org/

[10] IHO. 2017. International Hydrographic Organization . (2017). https://www.iho.int/

[11] IMO. 2017. International Maritime Organisation. (2017). http://www.imo.org/

[12] Inmarsat. 2015. *Iris Precursor Phase 1- Final Report*. Technical Report.

[13] ISO. 2015. Future Proof and Cost-Effective Standardization of Electronic Ship Certificates. (2015), 17 pages.

[14] ITU-R. 2015. *Technical characteristics for a VHF data exchange system in the VHF maritime mobile band*. Technical Report October. 1–54 pages.

[15] Maritime Connector. 2017. Container ship. (2017). http://maritime-connector.com/container-ship/

[16] Dag Atle Nesheim, Ørnulf Rødseth, Karin Bernsmed, Christian Frøystad, and Per Håkon Meland. 2017. *D1.1 Risk Model and Analysis*. Technical Report. SINTEF.

[17] Dag Atle Nesheim, Ørnulf Rødseth, and Per Håkon Meland. 2016. *D1.1a Context and user requirements*. Technical Report. SINTEF.

[18] Hannu Peiponen and Antti Kukkonen. 2010. Integrity monitoring and authentication for VDES Pre-Distributed Public Keys. (2010), 5 pages. http://www.iho.int/mtg

[19] M. Pini, L. Pilosu, L. Vesterlund, D. Blanco, F. LindstrÃűm, and E. Spaltro. 2014. Robust Navigation and Communication in the Maritime Domain: The TRITON Project. In *2014 IEEE Joint Intelligence and Security Informatics Conference*. 331–331. https://doi.org/10.1109/JISIC.2014.75

[20] Klaus Plößl and Hannes Federrath. 2008. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards & Interfaces* 30, 6 (2008), 390–397.

[21] S Santesson, M Myers, R Ankney, A Malpani, S Galperin, and C Adams. 2013. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. (2013), 40 pages. https://tools.ietf.org/html/rfc6960

[22] Brittany M. Thompson. 2014-1015. GPS Spoofing and Jamming: A global concern for all vessels. *Proceedings of the Marine Safety & Security Council, the Coast Guard Journal of Safety at Sea* 71, 4 (2014-1015).

[23] World Maritime News. 2014. IMB: Shipping Next Playground for Hackers. (2014). http://worldmaritimenews.com/archives/134727/imb-shipping-next-playground-for-hackers/