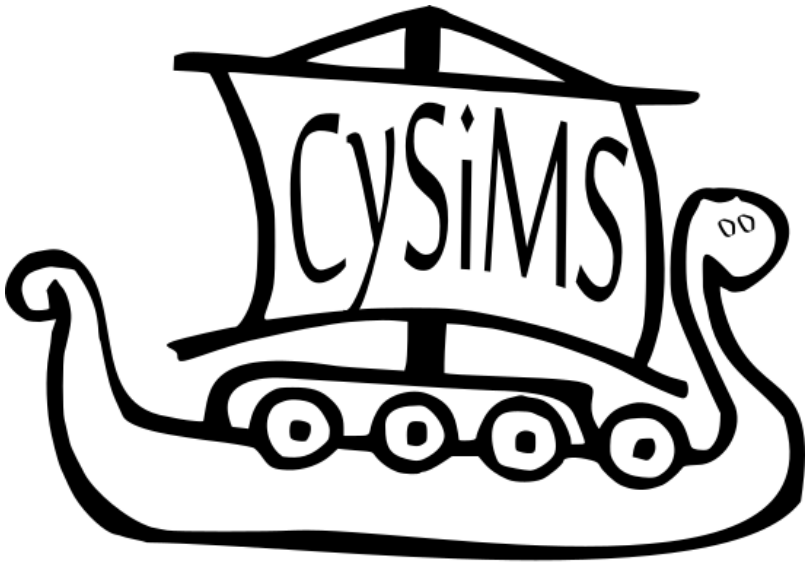
Unrestricted

Report

D2.2 Using digital signatures in the maritime domain

Authors
Christian Frøystad, Karin Bernsmed, Per Håkon Meland, Ørnulf Jan Rødseth, Dag Atle Nesheim



KONGSBERG
SINTEF
KYSTVERKET
Sjøfartsdirektoratet
Norwegian Maritime Authority
NAVTOR
DNV·GL
The Research Council of Norway

Report

D2.2 Using digital signatures in the maritime domain

KEYWORDS:
PKI, maritime, cyber security

VERSION
1.0

DATE
2017-03-31

AUTHOR(S)
Christian Frøystad, Karin Bernsmed, Per Håkon Meland, Ørnulf Jan Rødseth, Dag Atle Nesheim

CLIENT(S)
The Research Council of Norway

CLIENT'S REF.
256508/O80

PROJECT NO.
102013239

NUMBER OF PAGES/APPENDICES:
53

ABSTRACT

The CySiMS project aims to develop new security solutions that will provide integrated and cost-effective protection against cyber-attacks on critical safety and operational information in the maritime domain. This document presents a Public Key Infrastructure (PKI) for maritime communication, which can be used to secure ship-to-ship, ship-to-shore and shore-to-ship communication. A key design goal has been to adapt the solution to the maritime domain where bandwidth is limited and where ships may be offline during long periods. In addition, international applicability and a cost-efficient operation of the solution have been important drivers. In this document, we outline the design of the PKI, explain how it can be operated and propose some initial steps towards international acceptability and deployment through standardization.

PREPARED BY Christian Frøystad		**SIGNATURE** Christian Frøystad
CHECKED BY Martin Gilje Jaatun		**SIGNATURE**
APPROVED BY Arne Mikkelsen		**SIGNATURE**
ISBN 978-82-14-06161-1	**CLASSIFICATION** Unrestricted	**CLASSIFICATION THIS PAGE** Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2016-05-13	Initial version with Table of Content
0.2	2017-03-02	First draft version ready for internal review within consortium
0.3	2017-03-17	Second draft version ready for approval by the consortium
1.0	2017-03-31	Final version

Executive summary

Maritime communication is currently undergoing major changes. The transition from analogue voice over VHF-radio to digital messages over VHF Data Exchange System (VDES), and the introduction of Satellite Communication (SATCOM) as an additional communication channel, means that the stress on the current communication links are reduced and new services can be introduced. When technology continues to develop, the importance of cyber security to ensure safe and reliable operations is increasing.

This document outlines a Public Key Infrastructure (PKI) solution, which can be used to create, store and distribute cryptographic keys amongst a wide variety of users (including ships, shore stations, crew members and organisations) that will need to communicate securely, 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.

An overview of the proposed solution is as follows:

- Each of the involved actors (ships, services, organisations, etc.) will be equipped with cryptographic keys, which will be used to ensure confidentiality, integrity and authenticity of the transmitted information. The public cryptographic keys will be tied to their owners using X.509 certificates.
- The root of trust in the PKI ecosystem will consist of a Certificate Authority (CA), which should be operated by a trusted international organization, such as IMO. The responsibility of PKI management on the daily basis will be delegated to organizations operating on a national level.
- Ships will need to retrofit a dedicated PKI Unit to their bridge system. This unit can provide cryptographic services to both general and bridge network applications. The unit will utilize a smartcard for tamper-proof storage of the security credentials.
- The proposed solution includes processes for generating new X.509 certificates when actors are associated with new owners, and for invalidating X.509 certificates for cryptographic keys that have expired or that have been compromised.
- To reduce the stress on the communication links, ships will keep a local cache of relevant X.509 certificates, which can be updated when calling on a port.
- Shore-based actors will always have access to the latest version of all X.509 certificates, using a dedicated online server.
- The solution has been designed so that the security credentials that will be stored on-board the ships will have an expected lifetime around 20 years.

A key design goal has been to adapt the PKI solution to the specific characteristics of the maritime communication infrastructure, where bandwidth is limited and where ships can be offline at sea for long periods of time. Moreover, the proposed solution has been designed to be applicable in a global context and to fit with the existing roles and responsibilities of key stakeholders, such as the International Maritime Organisation (IMO), Flag States and their Recognized Organization, Port State control, Ship-owners, crew members on board the ships, 3rd party Service Providers and any other entities that will need to communicate securely. Finally, we have considered the need for the PKI solution to be cost efficient, to be retrofittable to existing bridge systems and easy to operate for on-board crew without any specific technical knowledge.

Table of contents

1 Introduction

The European maritime sector and infrastructure is critical to the world economy. Even though maritime activities are relying more and more on ICT, the awareness on cyber security threats to the maritime sector is currently very low [1]. On the other hand, history shows that the threat of maritime terrorist attacks is real, e.g. Achille Lauro in 1985 [2], Limburg in 2002 [3] and Superferry 14 in 2004 [4]. These incidents were all physical attacks on the ships and their passengers, but it is only a matter of time before cyber-attacks will be part of the terrorists' arsenal.

The main objective of the "Cyber Security in Merchant Shipping" (CySiMS) project[1] is to develop new maritime security solutions that provide integrated and cost-effective protection against cyber-attacks on critical maritime safety and operational information, while contributing to and making use of emerging specifications and standards.

1.1 CySiMS Overview

CySiMS aims at improving the communication infrastructure of the maritime sector, as well as establishing the necessary groundwork for providing digital signing of, e.g., ship certificates. The main focus is to create a solution that works with the proposed VHF Data Exchange System (VDES) technology [5] which also includes the Automatic Identification System (AIS) communication channels. However, the aim is that the solution will be sufficiently general and extensible, enabling adoption for other purposes and communication links as well. As we are working on technology that will not be widely available and defined before 2021, we base the use cases on the future Maritime Service Portfolio (MSP) [6] and other envisioned services rather than the current situation.

As can be seen in Figure 1, future maritime communication will cover a diverse set of interactions, including information exchanges between ships, ships and organisations (such as ports, Vessel Traffic Services, and Shipping Operation centre), and ships and services (such as e-Navigation and Medical Aid Providers).

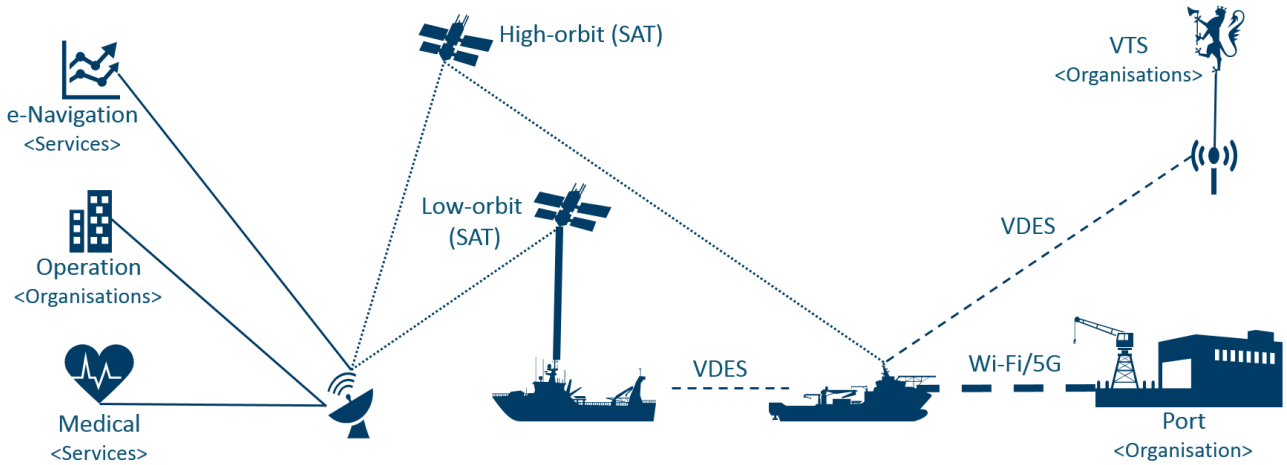


Figure 1 High level overview of the CySiMS ecosystem

The transition from analogue voice over VHF radio to digital messages over VDES, and the increased use of satellite communication (SATCOM), will lead to reduced stress on the current communication links and will

[1] The CySiMS project (2016-2018) is sponsored by the Norwegian Research Council. The consortium consists of DNV-GL, Kongsberg Defence and Aerospace, Kongsberg Gruppen, Kongsberg Seatex, Kystverket, SINTEF Ocean, Navtor, Sjøfartsdirektoratet and Stiftelsen SINTEF. See https://www.forskningsradet.no/prosjektbanken/#!/project/256508/en

enable new services to be introduced in the maritime domain. Which communication channel that will be used for which service, will depend on the ship's location, and the information to be transmitted.

The CySiMS security solutions will not be introduced into a vacuum but will need to coexist with the existing systems, networks and equipment that are already installed on the ships. Figure 2 shows a typical ship data network topology and communication links with different actors on shore. As illustrated in the figure, data enters the ship through communication channels such as VDES and SATCOM, and is routed through the different subnetworks, which are separated by firewalls.

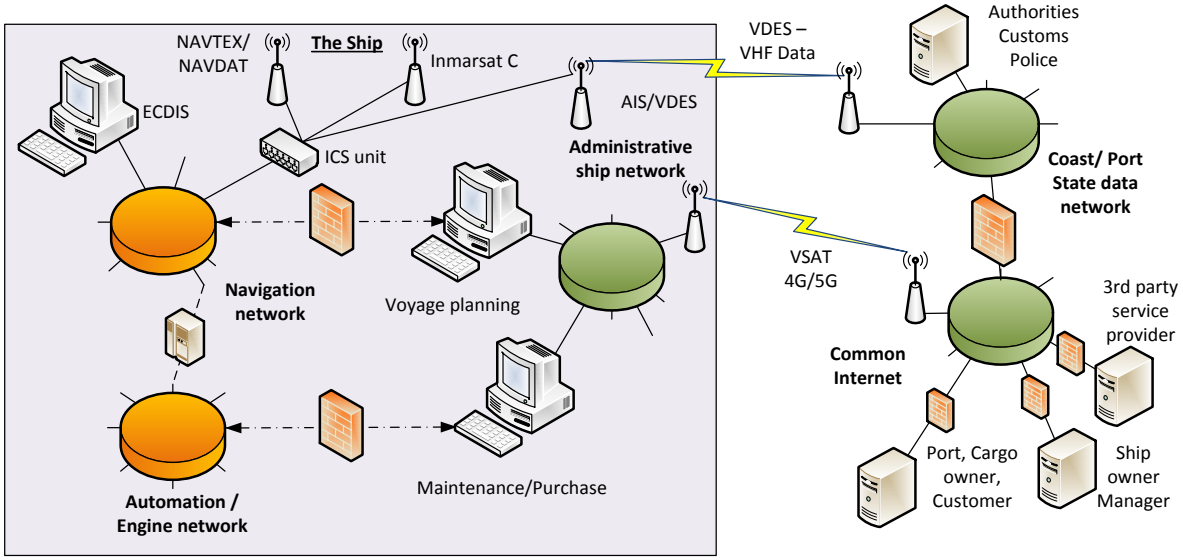


Figure 2 Typical ship data network topology

Note that an important component of a PKI is its *certificates*, which are used to verify that a public cryptographic key belongs to a specific user. These certificates must not be confused with ship certificates, which are used to demonstrate conformity to certain rules or standards w.r.t, e.g., load line, registry or passenger safety. To avoid confusion, we will therefore consistently use the term "X.509 certificate"[2] when we refer to the certificates associated with the PKI.

1.2 Structure of this document

The rest of this document is structured as follows. Section 2 presents the context that the security solution will operate in, the constraints that apply and the design goals that we have derived. In Section 3, we present the Public Key Infrastructure (PKI), including its trust hierarchy, necessary components, storage and processing units, the use of the X.509 certificate standard [7] and appropriate key materials and algorithms. This section also outlines the security services that the PKI should be able to support. In Section 4 we explain how the PKI will be operated, in terms of how to enrol users, how to use the X.509 certificates and how to handle expiration, renewal and revocation of the X.509 certificates. Finally, Section 5 concludes the report by suggesting a way forward using standardisation.

[2] The X.509 certificate standard [7] will be further described in Section 3.

2 The need for PKI in maritime communications

This section discusses the usage context and constraints of the PKI solution and outlines a set of design goals that the solution should meet.

2.1 Usage context

As was illustrated in Figure 1, CySiMS aims to handle a diverse set of interactions between ships and shore-based entities. To derive requirements for the PKI solution we have defined a number of high level use cases, which outlines how such interactions are envisioned to be implemented in the near future. These use cases are:

- **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 ships enters a foreign port.
- **UC3 Safety information**, which described the transmission of Maritime Safety Information such as 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 organisation instructions**, which refer to the messages exchanged between the ships and a VTS.
- **UC10 Telemedicine**, which covers remote communication between ships and medical aid providers on land.
- **UC11 Search and rescue**, 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 is related to broadcasts of data on how VDES is used in a certain area. Missing this data may mean that all or parts of VDE transmissions may be lost.

These use cases are further described in the CySiMS project deliverable "D1.1 Risk Model and Analysis" [8]. The D1.1 deliverable includes a threat and risk analysis of these use cases, which identifies the cyber security attacks the actors involved in the use cases may face, and the likelihood and impact of such attacks.

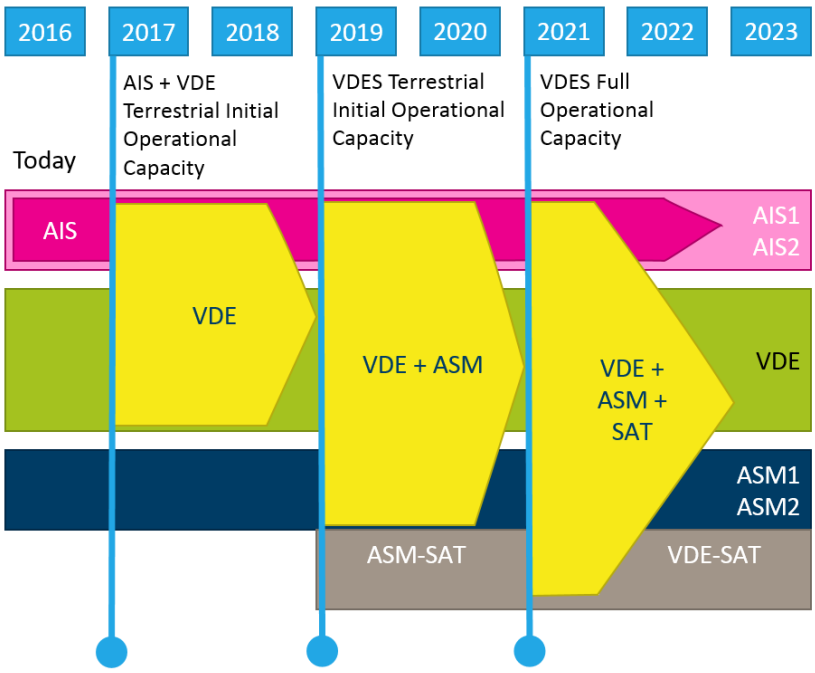


Figure 3 The Roadmap for VDES according to IALA[3]

The VDES technology, which is the main communication system in focus in this deliverable, is still under development. Figure 3 shows the roadmap to completion and full operational capacity by 2021, at which time VDES will encompass Automatic Identification System (AIS), VHF Data Exchange (VDE), Application Specific Message (ASM) and satellite based communication (SAT). The security solution presented in this document is designed according to the 2021 situation, but might be applicable to earlier stages as well.

The message structure for VDES has not yet been fully defined, but we can assume that the messages are likely to be rather short. Throughout this document, since the message structure for VDES is still in flux, it is assumed that a VDES message will have a rather limited payload, but 5 KB is not unrealistic. Furthermore, we assume that both unicast and multicast (broadcast) will be supported.

2.2 Needed security services

In Table 1, the use cases described in Section 2.1 are mapped to the security functionality they will require. The mapping is derived from an analysis of the use case characteristics and their associated cyber security risks, as described in the CySiMS deliverable D1.1 [8].

As can be seen, 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 or log books. The rest of the uses cases will require secure communication, where integrity of the transmitted messages stands out as the most important security functionality. Confidentiality protection will also be important in some scenarios, in particular for transmission of commercially valuable data, such as nautical charts (UC5) and voyage reports (UC6) and privacy sensitive data, such as passenger and crew lists (UC2, UC4) and medical information (UC10).

[3] Based on a draft document from 2016

Table 1 Mapping of high-level use cases to relevant security functionality. The use cases that utilize VDES are emphasized with light yellow 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 authority* → Port state authority				✓	offline	N/A
UC2 Single Window	Ship* ↔ Port state authority*	✓	✓	✓		SAT	U
UC3 Safety information	VTS*, MSI provider* → Ship	✓	✓			VDES SAT	M
UC4 Reporting	Ship* ↔ VTS*	✓	✓	✓		VDES	U
UC5 Nautical information	Ship* ↔ Nautical Service*	✓	✓	✓		SAT VDES	U
UC6 Operational exchange	Ship owner operations* ↔ Ship*	✓	✓	✓		SAT	U
UC7 Log book	Crew*				✓	offline	N/A
UC8 Traffic organization advice	Ship* ↔ VTS*	✓	✓			VDES	U
UC9 Traffic organization 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

In addition to required security functionality, Table 1 also outlines which communication channels the use cases will utilize. Since the main focus of our work is VDES, we will design the PKI solution so that it first and foremost meets the requirements of the use cases that will utilize VDES. The rows with these use cases have therefore been highlighted with light yellow colour in the table.

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", "Organisations", or "Individuals" – see Table 2 for details[4]. Ships and Services will need to communicate both over VDES and more general communication channels[5]. Organisations and Individuals will primarily use their keys for offline digital signatures of electronic documents.

Table 1 also outlines the need for authenticity, integrity and confidentiality protection of messages transferred over SATCOM (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 relatively short message transmissions, UC10 (Telemedicine) may require that a session of longer duration is established between the communicating actors.

Table 2 Overview of the needed security services per entity

Entity	Security service	Communication Channel	Justification
Ship	Message Authenticity	General VDES	The Ship requires message authenticity in UC2, UC4-6 and UC8-12 VDES is used in UC3-5, UC8, UC9, UC11 and UC12
	Message Integrity	General VDES	The Ship requires message integrity in UC2, UC4-6 and UC8-12 VDES is used in UC3-5, UC8, UC9, UC11 and UC12
	Message Confidentiality	General VDES	The Ship requires message confidentiality in UC2, UC4-6, and UC10 VDES is used in UC4 and UC5
	Secure session establishment	General	The Ship requires that a secure session, which provides message authenticity, integrity and confidentiality, is established in UC10.
Service	Message Authenticity	General VDES	The services require message authenticity in UC2-5, and UC8-11 VDES is used in UC2-5, UC8, UC9, and UC11
	Message Integrity	General VDES	The services require message integrity in UC2-5, and UC8-11 VDES is used in UC2-5, UC8, UC9, and UC11
	Message Confidentiality	General VDES	The services require message confidentiality in UC2, UC4, UC5, and UC10 VDES is used in UC2, UC4, and UC5
	Secure session establishment	General	The service requires that a secure session, which provides message authenticity, integrity and confidentiality, is established in UC10.

[4] Note that this is not intended to be an exhaustive list of all possible entities that will need to communicate, but a first draft. The scope can be extended at a later stage and thus introduce more entities

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

Entity	Security service	Communication Channel	Justification
Organization	Electronic Document Signature	Offline	The organisations require support for electronic document signature in UC1
Individual	Electronic Document Signature	Offline	Individuals require support for electronic document signature in UC7

2.3 Constraints

In addition to the high-level use cases, D1.1 Risk Model and Analysis [8] also describes a number of constraints that will affect the design of the PKI solution; the number of parties involved, the international dimension, the cost of implementing, deploying, operating and maintaining the PKI X.509 certificate hierarchy and the communication capacity of the network that will be used for ship-to-ship and ship-to-shore communication. Here we briefly summarize the constraints related to the cost and network characteristics related to the PKI solution. We also discuss applicable regulation.

2.3.1 Cost

International shipping is dependent on maintaining a reasonable and normally relatively low cost on its business operations and this imposes limitations on which solutions could be acceptable to the industry. The costs associated with implementing and operating the PKI solution must therefore be kept sufficiently low for its intended users, such as:

- Ship owners, managers and charterers
- Port state authorities and ports
- Flag states and their recognized organisations
- Operators of any security mechanisms included in the PKI solution

A variety of costs are imposed on several different actors in a value chain. There are costs related to the production of units, including design, testing, standardisation, manufacturing, and marketing. For the buyer, costs relate to procurement, installation, maintenance, operation and training. Different solutions will have different distribution of costs between the manufacturer and the buyer. In addition, there are costs related to operations for the relevant governmental organisations and service providers. All these aspects need to be considered when designing the PKI solution.

2.3.2 Network characteristics

The communication capacity is limited and it is therefore important to include both stress on communication links and the cost of using these links when designing the solution. Table 3 outlines the data capacity, cost and availability of the different communication links which will be used.

Table 3 Data capacity and cost of different data bearers

Communication link	Shared capacity	Cost	Availability
VDES	153.6 kbps	Free	Near shore, between nearby ships
GSM/LTE	100 Mbps	About 0.006 USD per MB[6]	Near shore
Low frequency (L-band), SATCOM	100 – 500 kbps	About 5 - 10 USD per MB[7]	Globally
High frequency SATCOM	100 kbps – 8 Mbps	About 1 - 2 USD per MB[8]	Globally, dependent on service provider
WiMAX/WiFI	10 - 100 Mbps	Free[9]	In port

Note that global availability depends on the satellite system. Iridium will in principle provide global coverage. Other SATCOM systems are today limited by the orbital position of geostationary satellites, i.e. normally limited to latitudes up to about 70 degrees north and south. SATCOM systems will also be limited by the specific satellite beam configurations.

The design must also consider the bit error rate (BER) of the communication link in order to ensure that the solution will work in its intended operational environment. Table 4 shows the probability that a package of a given length (left column) will contain at least one bit error at different BERs (first row). At the time of writing, we do not know what BER that can be expected for VDES. Is however likely that packet error rates that are less than 1% will be of little significance. In this deliverable, we will focus on the BER for VDES only, since satellite based communication channels have more capacity for error correction and resending packages than the somewhat limited VDES radio band.

Table 4 An overview over the packet error rates for different package lengths (PL) (left column in bytes) and bit error rates (BER) (first row). Courtesy of Hans Are Ellingsrud.

PL / BER	1,00E-08	1,00E-07	1,00E-06	1,00E-05	1,00E-04	1,00E-03
10	0,00 %	0,00 %	0,00 %	0,01 %	0,10 %	1,00 %
20	0,00 %	0,00 %	0,00 %	0,02 %	0,20 %	1,98 %
50	0,00 %	0,00 %	0,00 %	0,05 %	0,50 %	4,88 %
100	0,00 %	0,00 %	0,01 %	0,10 %	1,00 %	9,52 %
200	0,00 %	0,00 %	0,02 %	0,20 %	1,98 %	18,14 %
500	0,00 %	0,00 %	0,05 %	0,50 %	4,88 %	39,36 %
1000	0,00 %	0,01 %	0,10 %	1,00 %	9,52 %	63,23 %
2000	0,00 %	0,02 %	0,20 %	1,98 %	18,13 %	86,48 %
5000	0,00 %	0,05 %	0,50 %	4,88 %	39,35 %	99,33 %
10000	0,01 %	0,10 %	1,00 %	9,52 %	63,21 %	100,00 %

[6] 5 GB monthly plan at 249 NOK for use in Norway at https://www.telenor.no/bedrift/mobilt-bredband/
[7] 100 MB prepaid SIM for $525 USD at http://www.groundcontrol.com/BGAN_rate_plans.htm
[8] The Maritime VSAT Advantage: A cost analysis of VSAT broadband versus L-band pay-per-use service, iDirect
[9] Provided that the port offers such capabilities and includes any required maintenance costs in their ordinary port fees

2.3.3 Applicable regulation

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) [9]. 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 [10]. IMO instruments also includes 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 [11], 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 [11] 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 also result in various fees being payable. Errors or omissions in these reports can have direct economic consequences.

Finally, one also 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 is out of scope of this deliverable to include a complete study of applicable law in every part of the sea, but it is nonetheless 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 IMO and all its member states, so that it might be adopted by all relevant parties.

2.4 Design goals

This subsection outlines the design goals for the PKI solution. The design goals are derived from the usage context described in Section 2.1, the needed security services identified in Section 2.2, the constraints discussed in Section 2.3 and from internal discussions with the project consortium. The following goals have been identified:

1) **Secure information exchange**. 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) **Communication link independence**. The PKI solution should be independent of the communication link that is being used (VDES, SATCOM, WiFi, etc.).
3) **Ease of deployment and operation**. 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) **Offline cryptographic verification**. The cryptographic properties of the PKI solution must be verifiable offline – ships and inspectors are not always online.

5) **Low bandwidth needs**. The PKI solution must be adapted to the maritime communication infrastructure where bandwidth is limited.
6) **Low cost**. The costs of the PKI solution should be minimized.
7) **Global deployment and operation**. The deployment and operation of the PKI infrastructure, including enrolment, distribution and revocation of X.509 certificates, must be manageable in a global environment.
8) **Internationally acceptable**. The PKI solution must be acceptable in an international environment and fit with the existing roles, responsibilities and trust relationships of stakeholders in the maritime domain (IMO, flag states, coastal states, ship owners etc.).
9) **Compliance**. The PKI solution must be compliant with applicable legislations, regulations and standards worldwide.
10) **Cryptographic migration**. The PKI solution should enable migration to future cryptographic solutions without excessive costs or efforts.

Note that there already exist some solutions and ongoing work on PKI solutions for the maritime domain. The characteristics of these, and their applicability to CySiMS, are described in Appendix C.

3 PKI solution

This section outlines the design of the Public Key Infrastructure (PKI) that we propose. For reader unfamiliar with this topic, Appendix B provides a brief introduction to public key cryptography and PKI.

3.1 The PKI trust hierarchy

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

- A **Trusted international root Certificate Authority (CA)**, which will serve as the root of trust in the PKI hierarchy
- A number of **Issuing national CAs**, which will administrate X.509 certificates on a national level.
- **End entities**, which will be the ships, services, organizations and individuals that need to communicate securely (c.f. the needed security services identified in Section 2.2).

In addition, an entity called "CRL issuer", which will be 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. IMO is a candidate that fulfils these requirements[10]. Other potential candidates for operating the root CA are IALA[11], EMSA[12] or IHO[13].

The Issuing National CAs will, as the name indicates, be operated by organizations on a national level. A possible candidate for this role is the Flag State administration associated with each country.

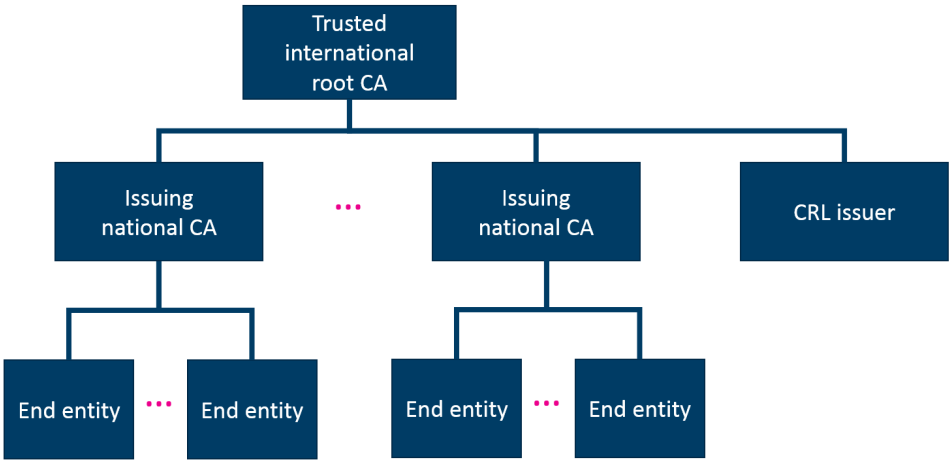


Figure 4 A general model of the PKI trust hierarchy

Figure 5 outlines an example of how the general model can be implemented, using Norway as a case study. In this example, the trusted international root CA is operated by IMO. The issuing national CA for Norway is

[10] IMO is already operating the root CA for the LRIT system[21]. IMO has also been proposed by ISO to act as the root of trust in a PKI for digital signatures of ship certificates [17].
[11] http://www.iala-aism.org/
[12] http://www.emsa.europa.eu/
[13] https://www.iho.int/

operated by the Norwegian Maritime Authority (*Norwegian: Sjøfartsdirektoratet*), which could manage the X.509 certificates for all the Norwegian end entities. Finally, the example provides some examples of end entities; one ship, one user, three services and four organizations.

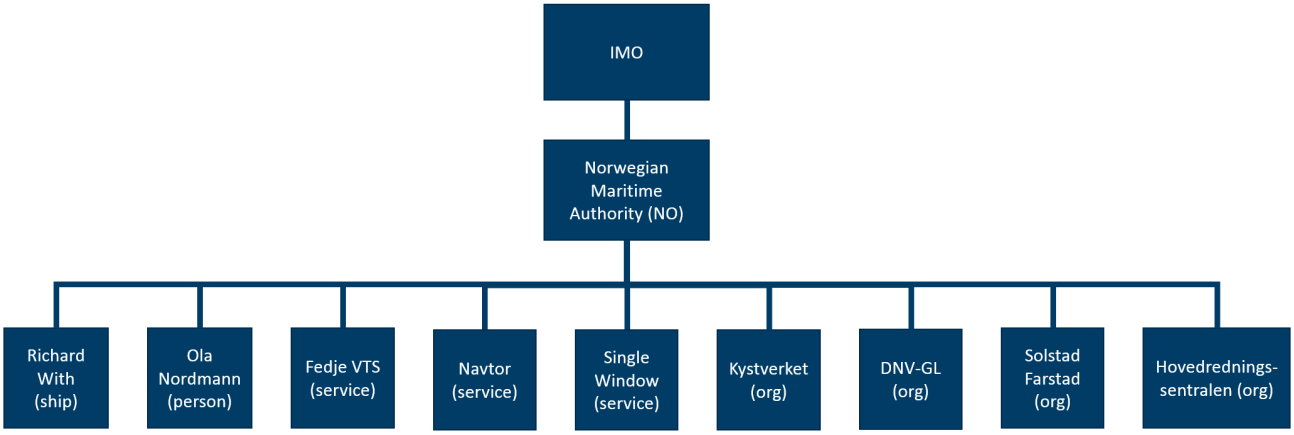


Figure 5 The PKI trust hierarchy from Figure 4 implemented in Norway

In Appendix H, we give an example of a scenario that involves the transition of end entities to new issuing national CAs in the trust hierarchy.

3.2 Components included in the PKI solution

An overview over the components necessary for operating the proposed PKI solution is illustrated in Figure 6. The figure includes the following components

- An air gapped **Root CA server**[14], 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 are used on-board the ships[15].
- **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 will be physically embedded in the PKI Units (cf. previous bullet point)[16]
- A **Smartcard inventory**, which keeps track of who possesses and owns each smartcard in the supply line and the end entities.

In the figure, dashed lines are used for logical connections (not online) and fixed lines are used for network connections (online). The thick blue line illustrates the use of the X.509 certificates to secure the connection between the end entities.

[14] The Root CA represents the root of trust in the PKI systemand 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.

[15] Appendix D outlines three potential options for installing the PKI on board the vessels, and concludes that a dedicated PKI unit will be the best choice.

[16] See Appendix E for a discussion on the use of smartcards and HSMs in the PKI solution.

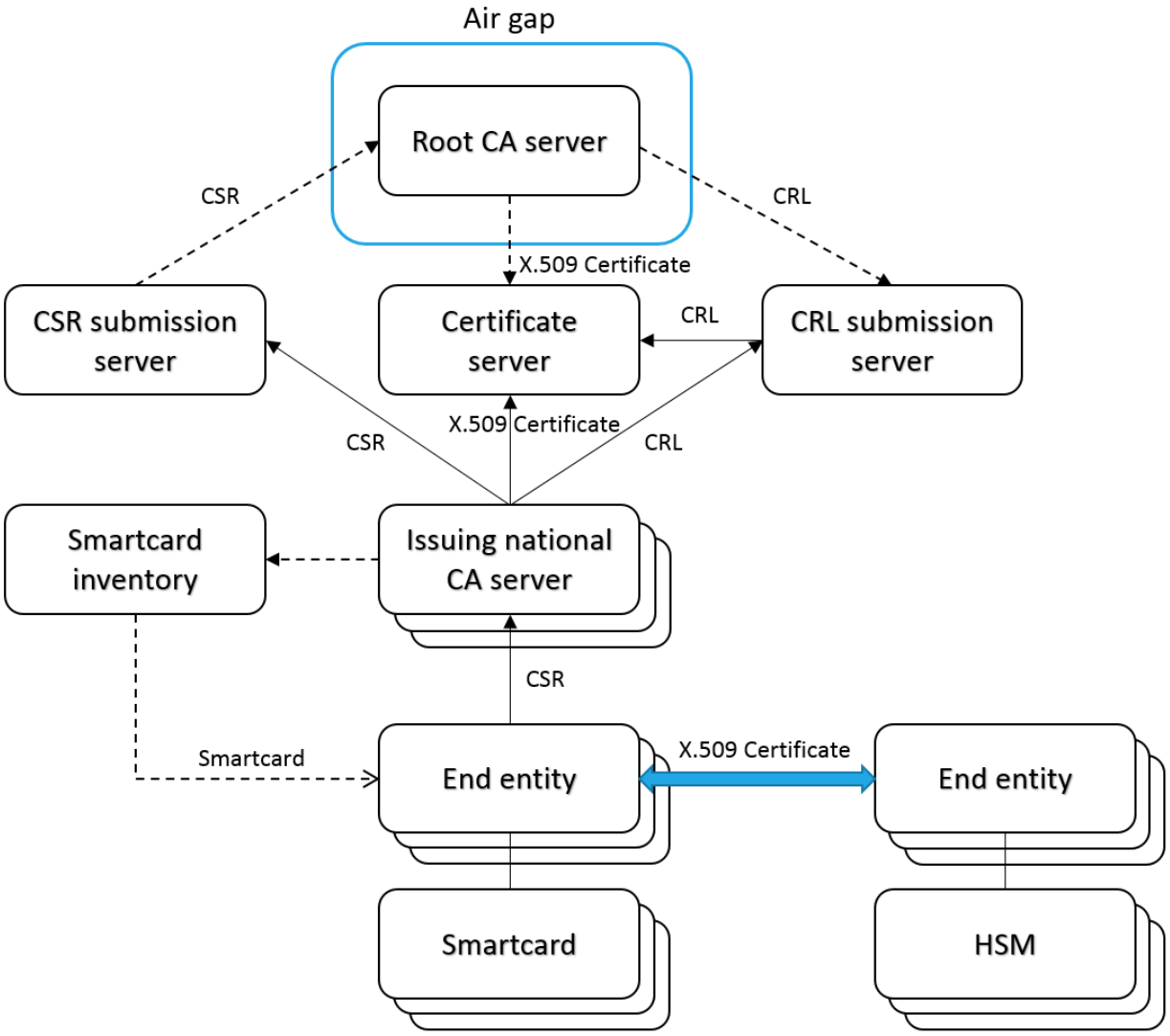


Figure 6 The main components included in the PKI system for secure maritime communication

The interactions between these components will be further described in Section 4 (Operational processes).

Each ship could have a PKI Unit, classified as navigational equipment and with an expected lifetime of 10 years. Figure 7 shows how the PKI Unit could be designed, with separate subsystems for general and bridge network usage. This way the X.509 certificates and smartcards can be made available to those who 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.

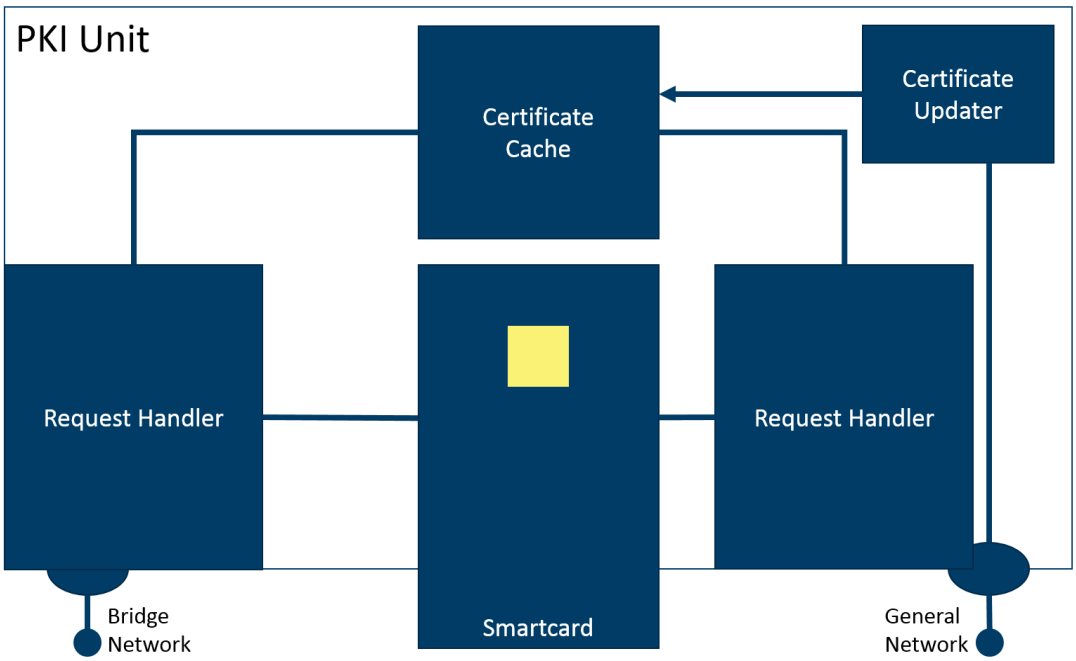


Figure 7 A logical example of how the PKI Unit could be designed with separate subsystems for general and bridge network usage

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.

The PKI Unit may require duplication if high availability is required. This may be needed, e.g. for ships that regularly need to send encrypted messages or to establish trusted sessions with shore entities or other ships. However, in most cases one can probably accept that one cannot sign messages for a limited time period and rely on other mechanisms in the cases where authentication is absolutely needed.

3.3 The X.509 certificate standard

The most established certificate standard for PKI is X.509 [7], which is commonly used for deploying certificate-based architectures on the Internet. This is also the standard we recommend for implementing a PKI for the maritime domain. The structure of an X.509 v3 certificate is shown in Table 5.

Table 5 The structure of an X.509 v3 certificate

Version	
Serial Number	
Signature Algorithm ID	
Issuer (CA) X.500 Name	
Validity Period	
Subject X.500 Name	
Subject Public Key Info	Algorithm ID
	Public Key Value
Issuer Unique ID	
Subject Unique ID	
Extension	
CA Digital Signature	

Most of the fields in an X.509 certificate (e.g. Version, Serial number, Signature Algorithm ID, etc.) will be generated automatically for each certificate request. However, the usage of some of the fields needs to be specified in order to fit the context of maritime communication. The **Subject X.500 Name** field will be used to uniquely identify the owner of the public key in the certificate. We propose the field to consist of the following information, dependent on whether the owner of the certificate is a ship, service, organization or an individual:

- The Common Name (CN) will be used to display the name of the entity (for e.g. a ship this would be the MMSI number). One can put almost anything in this field, as long as it is limited to 64 characters.
- The Organization (O) will be used to display the name of the organization that the entity is associated with
- The Country (C) will be used to indicate the country the end entity belongs to

As indicated in Table 6, we propose that ships are identified by using their Maritime Mobile Service Identity (MMSI) number[17]. Services, organizations and individuals can be identified by their names. Note that the Issuing national CAs and the Root CA will need to have specifically designed certificates that allow them to sign Certificate Signing Requests (CSRs) from other entities (cf. Figure 4).

Table 6 Subject X.500 Names for different types of X.509 certificates

Entity	**Subject X.500 Name**		
	Common Name (CN)	Organization (O)	Country
Ship	< insert MMSI number >	<insert organization ID + name, separated by ";">	< insert country code >
Service	< insert service name >		
Organization	< insert organisation name >		
Crew	< insert full name >		
Issuing national CA	<insert CA name >		
Root CA	< insert CA name >		

[17] The MMSI is a unique 9-digit number that is linked to the ship's flag and used as a unique communication identifier. It will change if the ship changes registry.

An example of a Subject X.500 Name for a ship X.509 certificate could be:

CN=232000000, O=NO948007029;SINTEF, C=NO

The **Issuer (CA) X.500 Name** field will be used to identify the owner of the public key in the CA certificate that will be used to verify the signature of the Subject's X.509 certificate. The Issuer Name field can be constructed in a similar manner as the Subject Name field.

In Appendix H, we give another example of Subject X.500 names for a ship and its owner.

3.4 Supported security services

Security services needed for the maritime domain were identified in Section 2.2. The following end entities were identified:

- Ships,
- Services,
- Organizations, and
- Individuals

A fundamental design principle of cryptography is to never use the same key pair for signing and encryption [12]. 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 keys used for, for example, authenticity and integrity protection of the mandatory reporting messages in UC4 (cf. Section 2.1) must therefore not be used to sign the electronic log books in UC7. It is will hence be necessary to maintain more than one key pair for some of the identified entities. In addition, we need to make sure that a certain key pair is only used for its intended purpose.

In the X.509 certificate standard [7], the "Key Usage" extension can be used to define the purpose of the key contained in the certificate. To be able to put usage restrictions of the key pair(s) that could be used for more than one cryptographic operation, we have therefore defined the following Key Usage extensions (Table 7):

Table 7 Key usage extensions for the X.509 certificates

Entity	Security service	X.509 Key Usage extension		Comment
		Critical	Key usage	
Ship	Message authenticity and integrity protection	Yes	digitalSignature, nonRepudiation	Keypair will be used to provide authenticity and integrity of messages transfers
	Message encryption	Yes	dataEncipherment	Keypair will be used to encrypt/decrypt messages transfers
	Secure session establishment	Yes	keyEncipherment, keyAgreement	Keypair will be used to establish a secure session over e.g. a SATCOM link.
Service	Message authenticity and integrity protection	Yes	digitalSignature, nonRepudiation	Keypair will be used to provide authenticity and integrity of messages transfers
	Message encryption	Yes	dataEncipherment	Keypair will be used to encrypt/decrypt messages transfers
	Secure session establishment	Yes	keyEncipherment, keyAgreement	Keypair will be used to establish a secure session over e.g. a SATCOM link.
Organization	Electronic document signatures	Yes	digitalSignature, nonRepudiation	Keypair will be used for generating/verifying/revoking digital signatures of electronic documents
Individual	Electronic document signatures	Yes	digitalSignature, nonRepudiation	Keypair will be used for generating/verifying/revoking digital signatures of electronic documents
Issuing national CA	PKI certification and revocation	Yes	keyCertSign, cRLSign	Keypair will be used to sign CSRs and CRLs
Root CA	PKI certification and revocation	Yes	keyCertSign, cRLSign	Keypair will be used to sign CSRs and CRLs

Note that defining a Key Usage extension as "Critical" means that any system using the X.509 certificates must reject the certificate if it encounters a critical extension that contains information that it cannot process [7].

3.5 Key material and algorithms

One of the trade-offs in designing a PKI solution is which length of keys to use for which length of time. The longer the keys, the longer they can be assumed to be secure, but longer keys will cause a larger overhead on the network, in addition to requiring more powerful processing systems.

Appendix F includes results from a study on suitable key material and algorithms for the maritime PKI solution that we have performed. Based on this study, we propose key lengths and algorithms for the root CA certificate, the issuing national CA certificates and the end entity certificates as indicated in the following subsections.

3.5.1 Key material and algorithm for the root CA

For the self-signed root CA certificate, a 4096 bit RSA key or equivalent ECC key should be used.

Our recommendation of cryptographic algorithm for the root CA digital signatures is the Elliptic Curve Digital Signature Algorithm (ECDSA) [13]. The ECC public key shall therefore be **384** bit. With this key size, the recommendations from RFC 5480 [14] states that the minimum bits of security should be **192**, the message digest algorithm **SHA-384**, and the curve **secp384r1**.

The lifetime of the selected key material is 20 years.

3.5.2 Key material and algorithm for the issuing national CA

For the issuing national CA certificates, a 2048 bit RSA key or equivalent ECC key should be used.

Similar to the root CA certificate, our recommendation of cryptographic algorithm for the issuing nation CA digital signatures is ECDSA. The ECC public key shall therefore be **256** bit. With this key size, the recommendations from RFC 5480 [4] states that the minimum bits of security should be **128**, the message digest algorithm **SHA-256**, and the curve **secp256r1**.

The lifetime of the selected key material is 10 years.

3.5.3 Key material and algorithm for the end entities

The end entities have different needs for protection, and thus also different keys will be needed for different purposes.

For the end entity certificates, a 2048 bit RSA key or equivalent ECC key should be used.

Our recommendation of cryptographic algorithm for the end entities digital signatures is ECDSA. The ECC public key shall therefore be **256** bit. With this key size, the recommendations from RFC 5480 [4] states that the minimum bits of security should be **128**, the message digest algorithm **SHA-256**, and the curve **secp256r1**.

The lifetime of the selected key material is 3 years.

An overview of the proposed key material and algorithms is provided in Table 8.

Note that, due to the limited bandwidth and potentially high BER 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 sufficient information is available. Some of the entries in Table 8 are therefore marked "*To Be Decided*" (*TBD*).

Table 8 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, keyAgreement	*TBD*	*TBD*	*TBD*
Organization	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

4 Operational processes

This section outlines how the Public Key Infrastructure (PKI) described in Section 3 will be operated.

The operation of the PKI will involve the following processes:

- Enrolment, in which an entity applies for and receives a signed X.509 certificate.
- Loading, in which the X.509 certificates are distributed and loaded to the ships.
- X.509 Certificate use, in which the entity uses a certificate for secure communication.
- X.509 Certificate expiration and renewal, in which certificates run out of date and are renewed.
- Revocation, in which X.509 certificates that are not valid anymore are revoked from the trust hierarchy.

These processes are described in Section 4.1-4.5, respectively.

The operational processes will involve the following actors:

- **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 will 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.

4.1 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.

4.1.1 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

The third step includes a secure out-of-band transfer of the CA certificate to the Smartcard Issuer, so that it can be installed on the smartcards during the ship enrolment process (see Section 4.1.3), 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 typical expected lifetime of the 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 communication equipment fails.

4.1.2 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 will 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.

4.1.3 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 will then be exported from the smartcards along with their sequence numbers and the serial numbers of the smartcards. This information will then be sent to the national Issuing CA Operator so that it will know which smartcards that will be 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[18] 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[19], which are illustrated in Figure 8:

- The PKI Sponsor orders a smartcard from the Smartcard Issuer[20] (step1).
- The Smartcard Issuer initializes 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 the relevant ship details to the Issuing CA Operator (step 5), which 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 will be sent to the Issuing CA Operator together with the activation code (step 8).
- The Issuing CA will 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).

[18] There could be more than one smartcard issuer as long as the integrity of the supply chain is preserved. The smartcards, along with information about which public keys belong to which smartcards, must be supplied to the relevant national issuing CA.

[19] For simplicity, the steps describe the enrolment of a single vessel into the PKI system. In reality, it is more likely that, for example, the PKI Sponsor will order a batch of smartcards and enroll multiple vessels simultaneously.

[20] Note that each vessel might carry several backup smartcards on board to ensure the continuing operation of the system in the event of a need to replace the smartcard

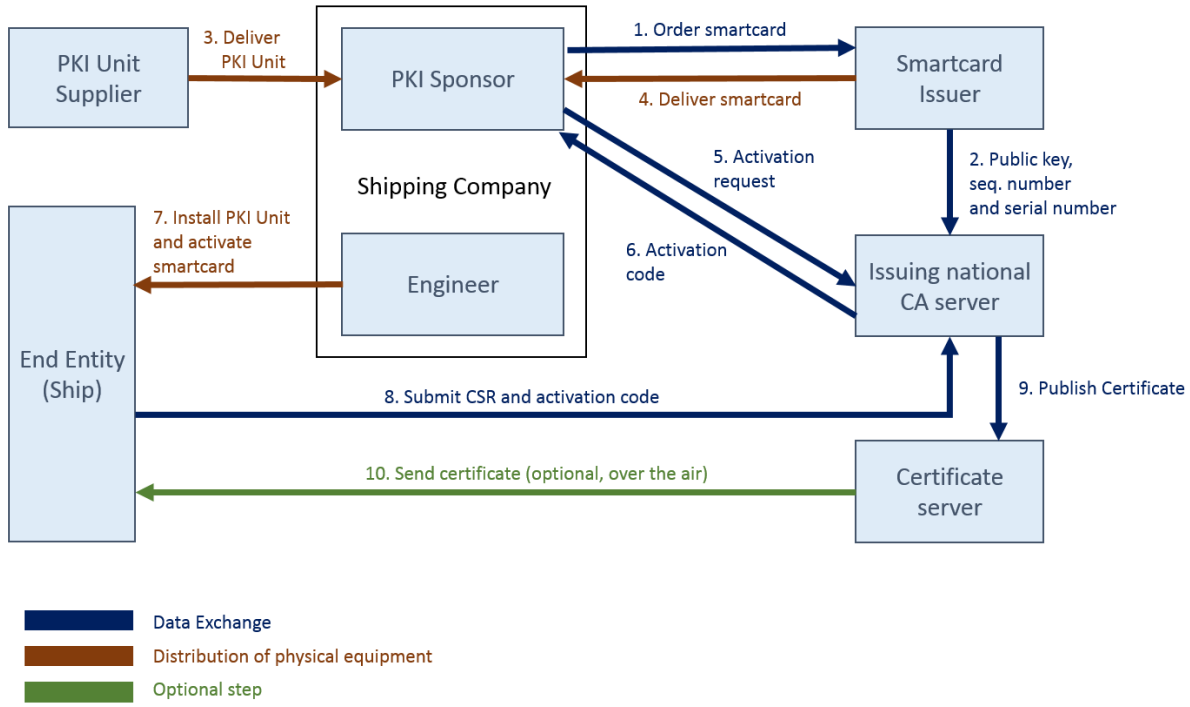


Figure 8 Enrolment of a ship into the PKI

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.

4.1.4 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. An example of an operational (prototype) solution is the Maritime Cloud Identity Platform described in Appendix C.6, which provides a web-based portal that can be used to request and issue new X.509 certificates.

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.

4.2 Loading the X.509 certificates onto the 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 will have a limited bandwidth when at sea.

We therefore propose that all relevant[21] 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 (see Appendix G for details), 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 at a port, the ship might not carry all the latest X.509 certificates at all times. This aspect has been discussed in the CySiMS consortium, which concluded that it is acceptable that both certificates occasionally may expire. 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. The actual implementation of the certificate exchange will be done by the application and is hence out of scope of this deliverable.

4.3 X.509 Certificate Use

Having access to the X.509 certificates of other entities, any enrolled entity can securely initiate operations requiring cryptographic protection. This section describes how these X.509 certificates will be used, by outlining how four of the security services identified in Section 3.4 will use the certificates:

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

Note that the services can be combined by applying a new service to the output of another.

4.3.1 Message authenticity and integrity protection

To achieve authenticity and integrity protection of a message that will be sent from a ship to e.g. a VTS (see Figure 9), the following steps will be performed:

1) The ship uses its private key to sign the message.
2) The signature is appended to the message and the signed message is sent to the recipient.
3) The VTS obtains the ship's X.509 certificate dedicated for message authenticity and integrity protection (from a cache or from the certificate server).
4) The VTS verifies that the obtained X.509 certificate is valid and has not been revoked
5) The VTS verifies the signature by using the public key of the ship, obtained from the X.509 certificate.

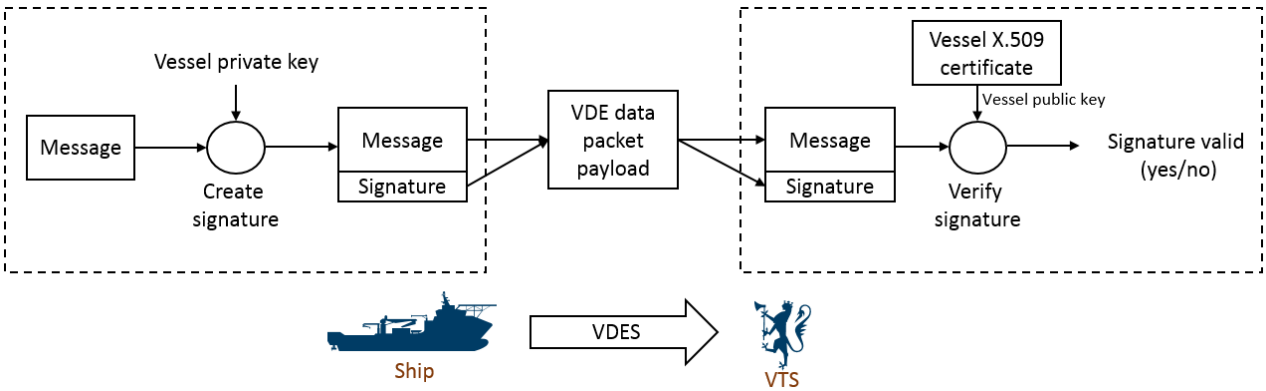


Figure 9 Authenticity and integrity protection of a message transmitted from a ship to a VTS.

[21] Which certificates that are relevant to cache is to be defined by the implementer of the solution.

4.3.2 Message encryption

To encrypt a message that will be sent from a ship to e.g. a VTS (see Figure 10), the following steps will be performed:

1) The vessel obtains the VTS X.509 certificate dedicated to encryption from the vessel's X.509 certificate cache
2) The ship encrypts the message using the public key in the VTS X.509 certificate
3) The encrypted message is sent to the recipient
4) The VTS decrypts the message using the private key corresponding to the public key used by the vessel when encrypting the message

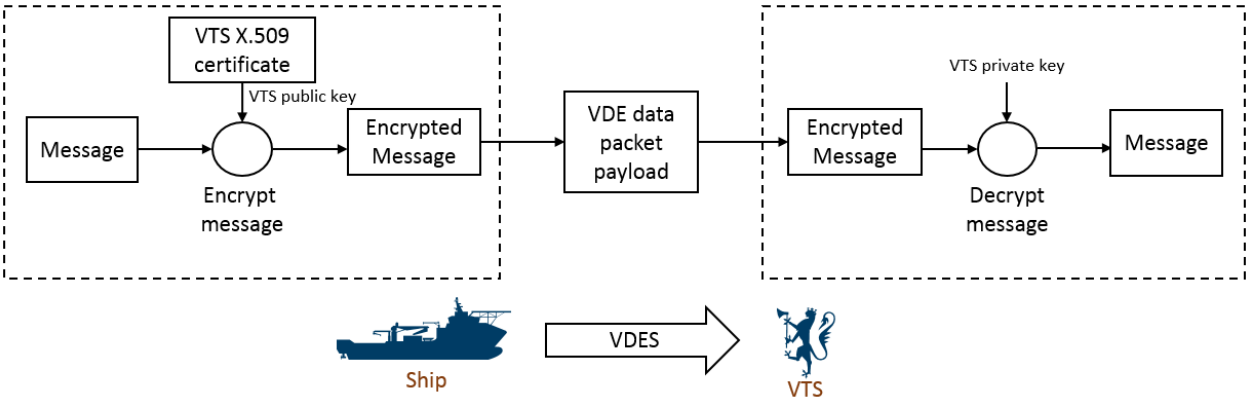


Figure 10 Encryption of a message transmitted from a ship to a VTS.

The approach outlined here (encryption and decryption using public and private keys) is not always a good choice, since it involves mathematically intensive computations. An alternative is to use the X.509 certificates to perform a key agreement procedure, in which the communicating entities agree on a symmetric key that can be used to encrypt and decrypt the message(s). This is outlined in the next subsection.

4.3.3 Secure session establishment

To establish a secure session, the communicating entities will use the public keys in each other's X.509 certificates (dedicated for secure session establishment) to perform a key agreement procedure (TBD which one), in which they agree on a shared symmetric key that is used to provide authenticity, integrity and/or confidentiality protection of all the messages exchanged in the session.

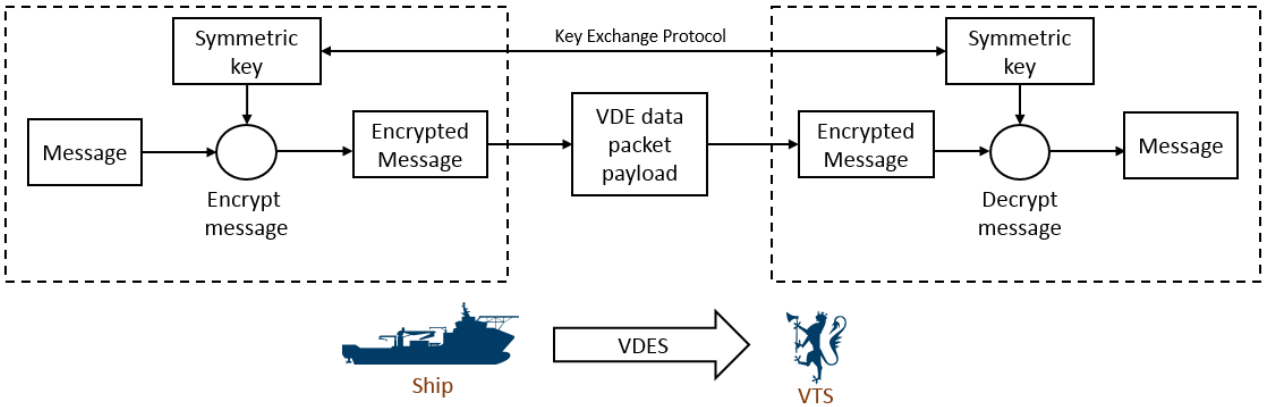


Figure 11 Encryption of a message using a symmetric key

As in the previous two examples, ships can either use the X.509 certificates in their caches, or they can request the other entity to send their X.509 certificate.

4.3.4 Electronic document signatures

In order to electronically sign a document (see Figure 12), the following steps will be performed:

1) The signing entity creates a hash of the document to be signed
2) The hash is signed by the entity's private key
3) Combine the signed hash and the public key into a document signature
4) The document signature is appended to the document to be signed

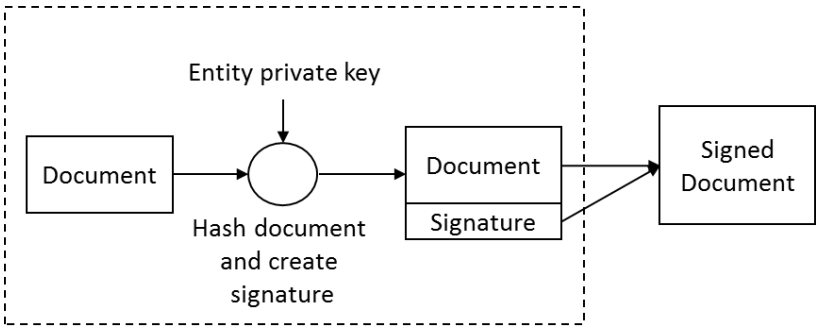


Figure 12 Electronic signature of document

4.4 X.509 Certificate Expiration and Renewal

As stated in Section 3.5, the validity period of the root CA certificate should be set to 20 years, the validity period of the issuing national CA certificates should be set to ten years and the validity period of the end entity X.509 certificates should be set to three years. Eventually, any certificate will therefore expire, and to prevent connectivity issues, there must be mechanisms in place for graceful renewal of all the certificates.

4.4.1 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[22] and run in parallel with the existing one. During this transition period, the root CA will sign all Certificate Signing Requests (CSRs) from the Issuing National CAs with both the old and the new X.509 certificate. All new smartcards that are produced during this transition period will 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 will 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

[22] 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 will 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 compromised by a malicious user.

will have a signature from the new Issuing National CA certificate, and the old Issuing National CA certificate can hence be retired.

End entities will 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 (cf. next subsection). Ship X.509 certificate renewal will be described in more detail in the next subsection.

The process is illustrated in Figure 13. The red lines illustrate which Root CA that will sign which Issuing National CA CSR and the orange line illustrates which Issuing National CA that will sign which end entity CSR.

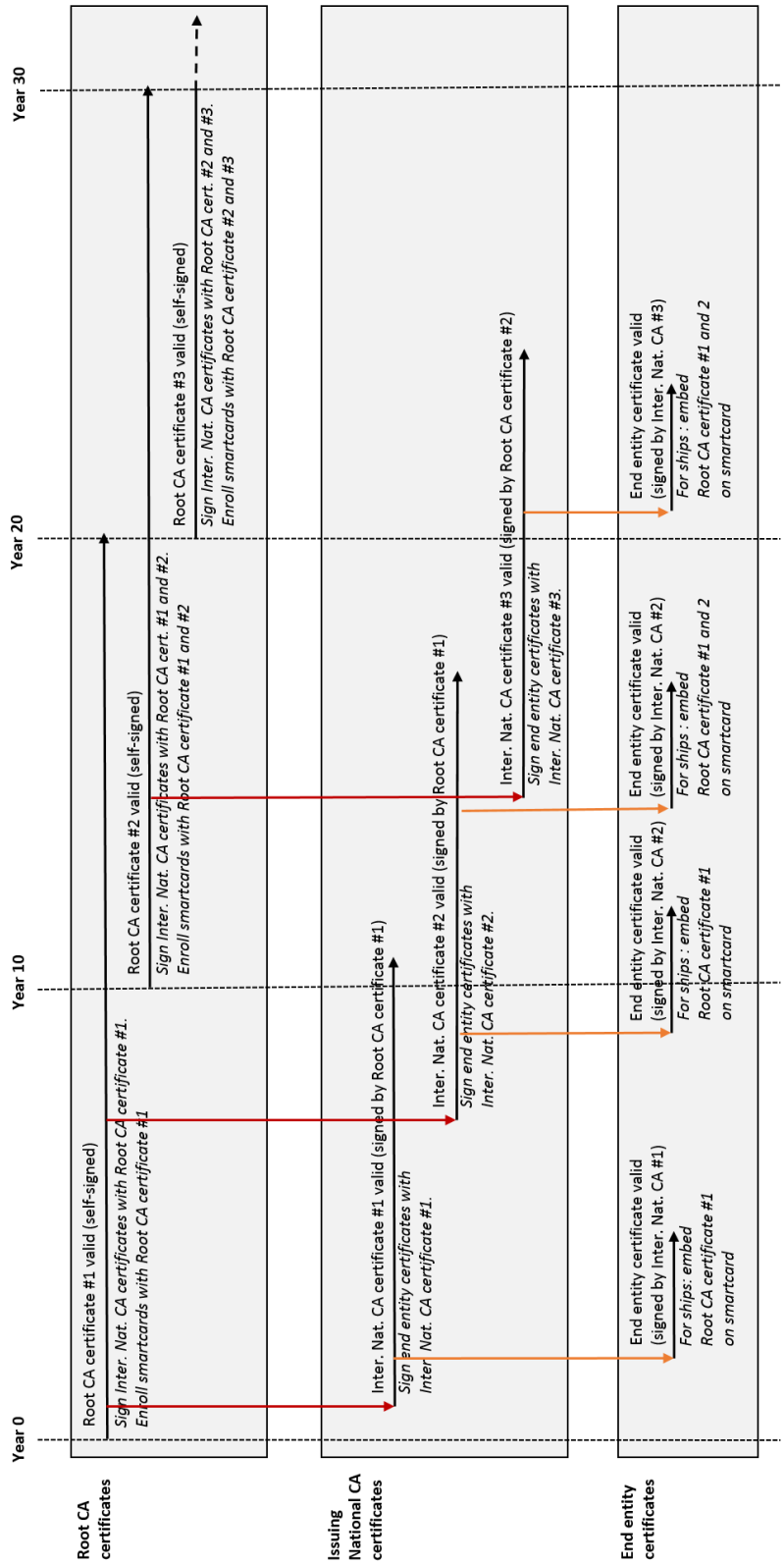


Figure 13 The X.509 certificate expiration and renewal process

4.4.2 Ship rekeying

To avoid having to replace the smartcards on the ships when the ships' X.509 certificates expire, rekeying will 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 will 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 enrollment process described in Section 4.1.3 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[23].

4.5 X.509 Certificate Revocation

A 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, transferred to another registry, or 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 [15][16], but rather build a scheme on the more offline suitable Certificate Revocation List (CRL) [7]. To keep the network traffic to a minimum, long lived CRLs combined with frequent delta CRLs will be used. Furthermore, the CySiMS consortium has discussed the loading of CRLs and agreed that it will be 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.

[23] An alternative to distributing new smartcards to all the vessel 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.

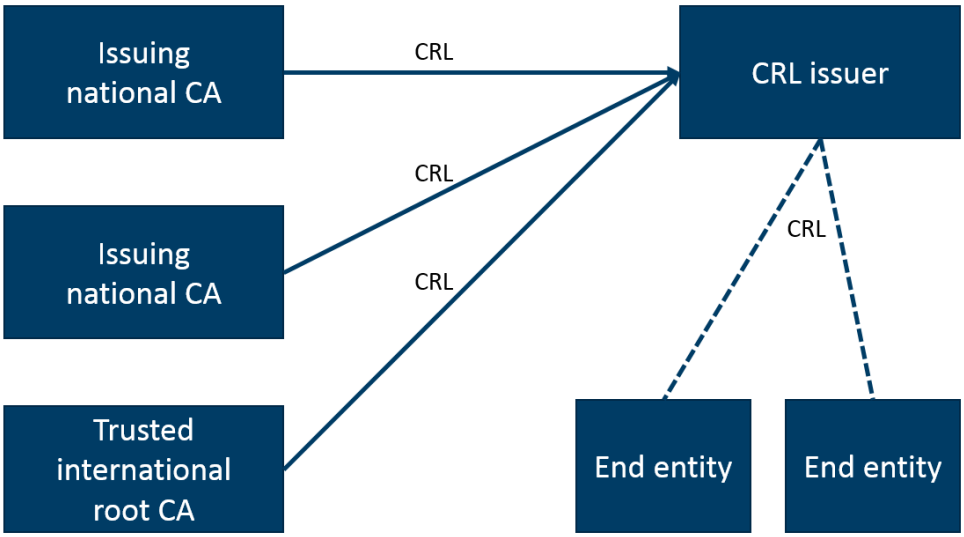


Figure 14 CRLs from multiple sources are collected and distributed through a CRL issuer

Figure 14 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 from the different issuing national CAs are handled on shore, giving entities a single source of CRLs and delta CRLs, rather than having each end entity fetch CRLs and delta CRLs from every issuing national CA. The CRL issuer is part of the certificate hierarchy on the same level as the issuing national CAs, as can be seen in Figure 4.

The PKI solution will 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 will be issued once a week after the same model as the CRLs

5 Summary and future work

This document has outlined a PKI solution, which can be used to create, store and distribute cryptographic keys amongst a wide variety of users in the maritime domain that will need to communicate securely in order to exchange critical information. The PKI can be used to 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. In this document, we propose the use of X.509 digital certificates to bind the cryptographic keys to the participating entities and illustrate how such a solution can be implemented in an international trust hierarchy. We also present a potential deployment alternative for storing and processing private keys and root CA X.509 certificates on board the ships. Finally, we have outlined how the enrolment and distribution of X.509 certificates to the ships, and revocation of such X.509 certificates, can be implemented.

For the solution to be adopted by the worldwide maritime community it needs to be standardized. As mentioned in Appendix I.A.1.a)(1)C, there are some ongoing work on standardizing security solutions for the maritime domain. For example, ISO TC8 has looked at how fully signed and electronic certificates can be implemented through a cooperation between IMO and the standards organizations [17].

The results presented in this deliverable is intended to be used as input to a standards process. An extended abstract of the document will therefore be compiled and sent to relevant national and international parties for feedback, and will be used as input to further discussions on security solutions for international maritime communication.

The initial steps towards international acceptability and deployment of the proposed PKI solution through standardization is as follows:

- March 2017: Finalization of the technical report including the design and operation of the PKI (i.e. this document)
- June 2018: Input paper to FAL on the design and operation of the PKI, based on the technical report

6 References

[1] ENISA, "Analysis for Cyber Security Aspects in The Maritime Sector," 2011.

[2] History.com, "Achille Lauro hijacking ends," *History.com*. [Online]. Available: http://www.history.com/this-day-in-history/achille-lauro-hijacking-ends. [Accessed: 21-Oct-2016].

[3] BBC News, "Yemen says tanker blas was terrorism," *BBC News*, 2002. [Online]. Available: http://news.bbc.co.uk/2/hi/middle_east/2334865.stm. [Accessed: 21-Oct-2016].

[4] BBC News, "Bomb caused Philippine ferry fire," *BBC News2*, 4AD. [Online]. Available: http://news.bbc.co.uk/2/hi/asia-pacific/3732356.stm. [Accessed: 21-Oct-2016].

[5] ITU-R, "Technical characteristics for a VHF data exchange system in the VHF maritime mobile band," 2015.

[6] Kystverket, "Safety and Navigation using e-Navigation solutions." .

[7] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "RFC 5280- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2008. [Online]. Available: https://www.ietf.org/rfc/rfc5280.txt. [Accessed: 06-Sep-2016].

[8] "D1 1 Risk Model and Analysis." .

[9] UNCLOS, "United Nations Convention on the Law of the Sea." [Online]. Available: http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf. [Accessed: 27-Feb-2017].

[10] The International Maritime Organization (IMO), "GUIDELINES FOR THE USE OF ELECTRONIC CERTIFICATES." 2016.

[11] Samferdselsdepartementet, "Forskrift om fartøys meldeplikter etter havne- og farvannsloven - Lovdata." [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2015-12-21-1790. [Accessed: 22-Mar-2017].

[12] E. Barker, "NIST Special Publication 800-57 Part 1 Revision 4 Recommendation for Key Management."

[13] "RSA Laboritories. PKCS #13: Elliptic Curve Cryptography Standard." [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-13-elliptic-curve-cryptography-standard.htm.

[14] S. Turner, R. Housley, T. Polk, D. R. L. Brown, and K. Yiu, "RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information." .

[15] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," *IETF*, 2013. [Online]. Available: https://tools.ietf.org/html/rfc6960. [Accessed: 19-Sep-2016].

[16] Y. Pettersen, "RFC 6961 - The Transport Layer Security (TLS) Multiple Certificate Status Request Extension," *IETF*, 2013. [Online]. Available: https://www.ietf.org/rfc/rfc6961.txt. [Accessed: 20-Sep-2016].

[17] ISO, "Future Proof and Cost-Effective Standardization of Electronic Ship Certificates," 2015.

[18] R. Shirey, "RFC 4949 - Internet Security Glossary, Version 2," *IETF*, 2007. [Online]. Available: https://tools.ietf.org/html/rfc4949. [Accessed: 01-Jan-2001].

[19] IMO, "LONG-RANGE IDENTIFICATION AND TRACKING SYSTEM TECHNICAL DOCUMENTATION (PART I)," 2014.

[20] IMO, "LONG-RANGE IDENTIFICATION AND TRACKING SYSTEM TECHNICAL DOCUMENTATION (PART II)," 2014.

[21] European Maritime Safety Agency (EMSA), "Annex 3 LRIT International Data Exchange (IDE) Functions and Architecture," 2013.

[22] EMSA, "ANNEX III Security Guidelines SafeSeaNet," 2013.

[23] International Hydrographic Organisation, "IHO Data Protection Scheme Edition 1.1.1," 2012.

[24] H. Peiponen and A. Kukkonen, "Integrity monitoring and authentication for VDES Pre-Distributed Public Keys," 2010.

[25] EfficienSea, “Deliverable 3.1. Analysis Report. Maritime communication and infrastructure Analysis,” 2015.
[26] EfficienSea, “Deliverable 3.2. Conceptual Model,” 2016.
[27] “RSA Laboratories. PKCS #1: RSA Cryptography Standard.” [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm.
[28] ENISA, “Algorithms, key size and parameters report - 2014,” 2014.
[29] NSA, “The Case for Elliptic Curve Cryptography,” 2009. [Online]. Available: http://web.archive.org/web/20090117023500/http://www.nsa.gov/business/programs/elliptic_curve.shtml. [Accessed: 06-Sep-2016].
[30] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, “Report on Post - Quantum Cryptography,” 2016.

A Abbreviations and glossary

AIS	Automatic Identification System
ASM	Application Specific Messages
ATS	Air Traffic Services
Authentication	Confirming the identity of an actor
BER	Bit Error Rate
C	Country
CA	Certificate Authority
Certificate Server	An online entity responsible for delivering X.509 certificates and certificate revocation lists (CRLs) on request to any entity in the system
CN	Common Name
Coastal State	Any nation with territorial rights to adjacent sea waters
CRL	Certificate Revocation List
CRL Cache	A local copy of the official CRL
CSR	Certificate Signing Request
CySiMS	Cyber Security in Merchant Shipping
DMA	Danish Maritime Authority
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithmic Problem
EMSA	European Maritime Safety Agency
Encryption	The process of transforming data, using some cryptographic function, to a state where it is unreadable and only a given key can reverse the process
Flag State	The nation which guarantees for the state and compliance with international regulations of the ship
GISIS	Global Integrated Shipping Information System
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
IDE	International Data Exchange
IHO	International Hydrographic Organization
IMO	International Maritime Organization
Integrity	The completeness and accuracy of data
Intermediate CA	Subordinate CA only issuing X.509 certificates to chid CAs
IS	Information System
Issuing CA	Subordinate CA issuing X.509 certificates to users, computers and services
ITU	International Telecommunication Union
LRIT	Long Range Identification and Tracking
MAP	Medical Aid Provider
MMSI	Maritime Mobile Service Identity
MRN	Maritime Resource Name
MW	Medium Wave
MSP	Maritime Service Portfolio
O	Organisation
OCSP	Online Certificate Status Protocol
OU	Organisation Unit
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number

PKI	Public Key Infrastructure
PKI Operator	The organisation in charge of maintaining and running the PKI
PKI Sponsor	The person, at any given organisation or company, responsible for interacting with the PKI Operator
PL	Packet Length
Port State	Any state that is not the Flag State of the ship in question
RA	Registration Authority
Revocation	The process of withdrawing a previously signed X.509 Certificate
RO	Recognised Organisation
RSA	Rivest, Shamir, and Adleman. Cryptographic algorithm
SAR	Search and Rescue
SAS	Satellite Anchor Station
SAT	Satellite Communication
SATCOM	Satellite Communication
SAR	Search and Rescue
SCC	Shipping Coordination Centre
Ship certificate	An official document published to prove that a ship, its equipment or other facets of the ship satisfies certain requirements
Signature	A cryptographic value generated by use of the private key belonging to the X.509 Certificate. The value is verifiable by means of the X.509 Certificate and ensures the authenticity and integrity of the data
SSL	Secure Sockets Layer
Subordinate CA	Any child CA
TLS	Transport Layer Security
USB	Universal Serial Bus
VDE	VHF Data Exchange
VDES	VHF Data Exchange System
VDL	VHF Data Link
VHF	Very High Frequency
VTS	Vessel Traffic Service
WiFi	Wireless network
WiMAX	Worldwide Interoperability for Microwave Access
X.509 Certificate	A digital X.509 certificate attesting to the identity of the holder and can be used in cryptographic functions

B A brief introduction to public key cryptography and PKI

This section includes a brief introduction to public key cryptography and Public Key Infrastructure (PKI), in order to make the deliverable more readable for those who are not familiar with cryptography.

Public key cryptography includes the use of two keys; a **private key**, which must remain a secret, and a **public key**, which can be shared widely. These two keys, which often are referred to as a **key pair**, are used to decrypt and encrypt data, respectively, and to sign and verify digital signatures. Public key cryptography can be used to provide data-origin and/or entity authentication, and data integrity, confidentiality and non-repudiation of data transfer.

A huge 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 often relies on **digital X.509 certificates**, which bind a public key of an entity to that particular entity. Note that the entity can be a user, a computer, a service or virtually any other device.

The goal of a **Public Key Infrastructure (PKI)** is to enable secure, convenient and efficient distribution of public keys through the use of digital X.509 certificates. A PKI is defined in RFC 4949 [18] as a set of hardware, software, people, policies and procedures that are needed to create, manage, store, distribute and revoke digital X.509 certificates based on public key cryptography.

A PKI includes the following key elements:

- **End entity**: a generic term used to denote any entity (end-user, server, router, etc.) that is the subject of a public key X.509 certificate and that is able to use the matching private key.
- **Certification Authority (CA)**: a generic term used to denote an entity that issues digital X.509 certificates, and usually also Certificate Revocation Lists (CRLs). Throughout this document, different names on the CA will be used to denote the concept depending on its role. The *root CA* is the root of trust in the PKI infrastructure. The root CA will issue a (self-signed) X.509 certificate to itself, and use this to issue certificates to one or more other entities in hierarchy. A *subordinate CA* is any child CA. An *intermediate CA* is a CA that only issues certificates to child CAs, while an *issuing CA* is a CA that issues certificates to users, computers and services.
- **Registration Authority (RA)**: an optional component that is responsible for verifying that the information needed by the CA to issue X.509 certificates and CRLs is correct.
- **CRL issuer**: an optional component that a CA can delegate to publish CRLs
- **Repository**: a generic term used to denote any method used for storing X.509 certificates and CRLs so that they can be retrieved by the end entities

A X.509 **certificate chain** will consist of all the certificates needed to validate an end entity's certificate. In practice this includes the entity certificate, the certificates of (all the) subordinate CAs and the certificate of a root CA.

Additionally, in this report the term **PKI Operator** is used to describe the organisation in charge of maintaining and running the PKI, while the term **PKI Sponsor** is used to describe the person, at any given organisation or company, responsible for interacting with the PKI Operator.

To set up and operate a PKI a number of management functions need to be supported:
Registration is the process where an end entity make itself known to the CA. **Initialization** includes generating the key materials (one or more public and private key pairs). **Certification** is the process where

the CA issues a X.509 certificate for the end entity's public key, returns the certificate to the end entity and/or stores it in a repository. **Key pair recovery** includes a mechanism for allowing end entities to restore their key pair from an authorized back-up facility in case of loss. **Rekeying** includes replacing an existing key pair with a new key pair and issuing a new certificate. Rekeying is used when either the current certificate expires or as a result of certificate revocation. **Revocation request** is the process when an authorized person advises the CA to revoke a certificate, for example if the private key has been compromised or if there is a need for a change of any of the fields (e.g. name or affiliation) in the certificate.

C Existing PKI solutions for the maritime domain

This appendix presents existing solutions and ongoing work on PKI solutions for the maritime domain.

C.1 LRIT security

The long-range identification and tracking (LRIT) system [19] [20] is used to transmit information (identity, position and date & time) from ships to Flag States, Coastal States, Port States and SAR authorities. LRIT has been developed under the co-ordination of IMO and is available to IMO Contracting Governments.

The LRIT International Data Exchange (IDE) is responsible for routing of messages between the LRIT data centers, and can be seen as the communication hub of the LRIT network. The LRIT IDE components use TLS to set up a secure communication channel (providing confidentiality and integrity protection), which uses a PKI for authentication. The LRIT IDE is hosted and operated by European Maritime Safety Agency (EMSA) [21] and the LRIT PKI is managed by IMO.

Highlights from the LRIT security solution:

- ➔ IMO is already operating a world-wide maritime PKI
- ➔ Digital certificates are used for device authentication in the LRIT communication network

Applicability to CySiMS: The LRIT PKI solution is mature, but has a different, and much smaller, scope than we are targeting in this project. The existing solution is unlikely to be extendable to meet all the CySiMS design goals, however, IMO might be willing and able to operate the CySiMS PKI as well.

C.2 The SafeSeaNet

The SafeSeaNet (SSN) is a ship traffic monitoring and information system operated by EMSA[24]. It has been set up as a network for maritime data exchange, and is based on monitoring Automatic Identification System (AIS) broadcasts from ships. SafeSeaNet currently covers all European coastal waters.

SafeSeaNet implements an XML messaging system, which uses SSL/TLS to protect the communication channel. EMSA operates a PKI, which is used to issue (and revoke) certificates for national SSN systems. Application servers that send SSN data are provided with client certificates and web/application servers that receive SSN data are provided with server certificates. The EMSA PKI is based on the X.509 standard [22].

Highlights from the SafeSeaNet security solution:

- ➔ EMSA is already operating a European-wide maritime PKI
- ➔ Digital certificates are used for device authentication in the messaging system

Applicability to CySiMS: The SafeSeaNet PKI solution is mature, but has a different, and much smaller, scope than we are targeting in this project. The solution is unlikely to be extendable to meet all the CySiMS design goals. EMSA might not be the right candidate for operating a world-wide PKI.

C.3 The IHO Data Protection Scheme

International Hydrographic Organization (IHO) S-63 [23] is a standard for securing electronic nautical charts (ENCs), which has been adopted by most commercial producers.

The standard relies on a PKI, in which the International Hydrographic Organisation (IHO) operates as the root CA. IHO is responsible for generating and distributing key pairs to the ENC producers, which use it to sign and encrypt the charts that they produce, and to the original equipment manufacturers (OEMs), which

[24] http://www.emsa.europa.eu/ssn-main.html

use it to sign and produce licenses for the software they deliver. The root CA public key is typically preloaded into the equipment by the OEM before the equipment is delivered to the end-users. The IHO PKI uses X.509 v3 certificates. Two independent methods can be used by the end-users to verify the charts and their updates: the X.509 files can either be loaded directly into the equipment, or one can manually input the character string that represents the public key.

Highlights from the IHO data protection scheme:

- ➔ IHO is already operating a PKI, which is based on the X.509 certificate standard
- ➔ The PKI is used to protect the integrity of ENCs and to implement software licenses

Applicability to CySiMS: The ENC PKI solution is mature, but has a completely different scope than we are targeting in this project. The solution does not fit the CySiMS design goals.

C.4 Ongoing work on digitally signed ship certificates in ISO

ISO/TC 8 Ships and marine technology has investigated how digitally signed ship certificates[25] can be standardized in the maritime domain, and propose to use a PKI to implement this [17]. In ISO's proposal, ship certificates will be produced by a flag state (FS) or by a recognised organisation (RO), by populating a ship certificate template that will then be signed by the FS's, or RO's, private key. The electronic signatures can then be verified by an inspector by means of computer, tablet or smart phone. ISO proposes that IMO operate as the root CA and be responsible for generating private keys and issue certificates for the FSs. The FSs will then issue certificates for their ROs in a hierarchical manner.

In their report [17], 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. GISIS[26], which will make it easier to retrieve and revoke certificates. Further, ISO suggest that the proposed solution could also be applied to other areas where authentication of digital information is needed, for example e-navigation, but points out that including ships in the PKI will dramatically increase the number of keys / certificates involved.

Highlights from ISO's work on electronic signed ship certificates:

- ➔ ISO is ready to support standardization of a digital signature solution, which includes setting up an international PKI operated by IMO
- ➔ ISO takes on a positive view towards a common PKI solution for securing ship certificates, e-navigation and other future application areas in the shipping sector

Applicability to CySiMS: The scope of the ISO/TC 8 work is narrow, but highly relevant for CySiMS and we should synchronize with their work when developing our proposal. The CySiMS D2.1 and/or D2.2 deliverables may serve as input to the ISO standardization process.

C.5 Ongoing work on VDES security in IALA

A recent working document from an IALA committee [24] 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, shore-to-ship and ship-to-ship application data.

[25] "Ship certificates" must not be confused with "PKI certificates" (the focus of this deliverable). The difference is that ship certificates are used to demonstrate conformity to certain rules or standards w.r.t, e.g., load line, registry or passenger safety whereas PKI certificates are used to verify that a public key belongs to a particular user.
[26] Global Integrated Shipping Information System. https://gisis.imo.org/Public/Default.aspx

Further, they propose that public keys can be distributed over any standard maritime communication means, including VDES. The committee concludes that more work is needed to decide 1) how simultaneous handling of multiple keys for shipborne VDES applications should be handled, 2) how to input public keys into VDES applications when the keys are received by other communication means than VDES, and 3) how the PKI infrastructure should be set up and operated.

Highlights from IALA's work on VDES security:

- ➔ The physical deployment of a PKI solution (private keys and root CA certificates) on-board ships is still an unsolved problem.
- ➔ IALA outlines the implementation of application specific PKIs as a potential alternative

Applicability to CySiMS: The scope of the IALA document is highly relevant for us and it corresponds with most of our design goals. We should synchronize with their work when developing our proposal. The CySiMS D2.1 and/or D2.2 deliverables could serve as input to the IALFA committee, in particular regarding alternatives for the physical deployment of the PKI solution.

C.6 Ongoing work on identity management in the Maritime Cloud

The Danish Maritime Authority (DMA) has implemented a Maritime Cloud identity platform, which is intended to serve as a solution for worldwide identification in the maritime community. The platform includes a PKI solution for authentication, which can be used to identify any type of entity, including vessels, devices (e.g., servers), services, organisations or end-users (humans). The DMA has implemented a web-based portal[27] where organisations can log in, create an X.509 certificate signing request, which will then be signed by the Maritime Cloud CA. The portal can also be used for revoking certificates and for downloading certificate revocation files. The Maritime Cloud platform currently operates its own root CA, but foresees that in the future every Flag State would have its own intermediate CA.

The Maritime Cloud identity platform is a result from the EU project EfficienSea2[28] [25][26].

Highlights from the Maritime Cloud identity platform:

- ➔ The Maritime Cloud identity management solution includes all types of potential entities; vessels, devices, services, organisations and users
- ➔ The DMA has already implemented a prototype PKI solution based on the X.509 standard

Applicability to CySiMS: The Maritime Cloud identity platform is highly relevant for the CySiMS project and their PKI solution meets some of our design goals. Their prototype could potentially be used to demonstrate some of the key aspects of the CySiMS PKI solution.

[27] http://developers.maritimecloud.net/identity/index.html
[28] http://efficiensea2.org/

D Ship Cryptographic Solution

Regarding the installation of smartcards on ships, several potential solutions exist, including

- Embedding the smartcard into the VDES unit
- Developing a dedicated PKI unit
- Using a conventional bridge computer

Embedding the smartcard into the VDES unit would mean that the VDES unit must make the smartcard security functionality available to other units on the bridge, so that the ship authentication credentials can be shared between the systems on board. An advantage of this would be that no additional hardware (except the VDES equipment) needs to be purchased and installed on the ships. Even though this is feasible solution, it is unlikely to be supported by the IALA e-NAV Committee, since their current view is to keep security out of the VDES standard.

Developing a dedicated PKI unit would ensure that all applications and communication systems have access to the PKI at the same level and would not have to rely on a potential competing technology. Additionally, it would serve only one purpose, which would simplify the access control across network barriers. If created as a network appliance with two ports, which form separate internal systems, but share the smartcard, systems in the secure bridge network and systems outside can use the same smartcard and unit without interfering with each other. The downside is the additional cost of purchase, installation and maintenance of the PKI unit.

Using a conventional bridge computer is a flexible and cost effective approach, with regard to new equipment, that would allow all systems and applications to access the PKI. The only additional equipment that needs to be purchased is a smartcard reader. The downside is additional maintenance burden on the crew or the shipping company, which may require additional technical competence. Such a computer would need to be configured to offer the services of the cryptographic services to other appliances on the bridge, but also to systems outside the closed bridge network. This would require diligence and competency both during initial configuration and future maintenance in order to ensure the security of the bridge network and the specific computer offering the service.

CySiMS proposes: a separate network unit which offer cryptographic services through one smartcard, but have separate subsystems for the bridge and general network. Both subsystems offer the same API

E Storage and processing units

To ensure security in a PKI architecture, all the private keys need to be properly protected. In addition, the root CA certificate(s), which represents the trust anchor in the system, needs to be protected from unauthorised modification.

There are different options for where to store and process private keys and root CA certificates in a PKI ecosystem. A **smartcard** is a pocket-size card with embedded integrated circuits. A smartcard provides a tamper-resistant security system and has built-in processing capabilities that can perform cryptographic functions. The smartcard can therefore be considered to be a *trusted hardware platform*. However, the hardware resources of smartcards are limited; the security system is facing the constraints of memory capacity and computing power. PKI-enabled smartcards are commonly used for strong authentication and application access control, often in combination a PIN code to access the private key(s) on the card. Additional advantages of smartcards are that they are inexpensive to purchase in large quantities, ensures secure storage of keys during transport to installation, and are easy to replace if broken.

CySiMS proposes: ship based entities (i.e. ships, and potentially also crew members on-board the ships) use smartcards for storing and processing the private key(s) and root CA certificate(s).

For shore-based entities (organisations and service providers), a **Hardware Security Module (HSM)** installed in the relevant servers is a simple solution, which will offer sufficient security. While a smartcard is a form of HSM, a larger, dedicated HSM has more storage and processing power making it capable of handling more keys, larger keys, and faster computation of signatures, encryption, decryption and signature verifications. Additionally, many HSM units employ extra logging and the possibility to automatically delete keys upon detecting tampering with the unit. PKI-enabled HSM are commonly used to enhance the security of a PKI infrastructure by providing secure storage of root CA certificates and private keys. A HSM is typically a PCI adapter but can also come in the shape of a network-based appliance.

CySiMS proposes: shore-based entities (organisations and service providers) use HSMs for storing and processing the private key(s) and root CA certificate(s).

Secure elements such as smartcards and larger HSMs provide functions such as key pair generation, secure storage of private keys and root CA certificates, and the execution of cryptographic operations. An alternative to smartcards and HSMs is to use a fully software based PKI approach, which would be very flexible with regard to the amount of available hardware, and with some additional measures it can be reasonable secure. However, a software solution has no secure storage of keys by default, and even if the key is protected somehow, it will still be available in memory during use.

F Cryptographic key material and algorithms

In this appendix, we present two potential public key algorithms for the maritime PKI solution, and discuss some of their strengths and weaknesses.

The two most prominent public key algorithms are Rivest-Shamir-Adleman (RSA) [27] and Elliptic Curve Cryptography (ECC) [13]. We have compared these using following three criteria:

1. Security: What is the security based on? How long has the cryptosystem been in wide use and how much has its security been studied?
2. Efficiency: How much computation is required to perform the public key and private key transformations? How many bits must be communicated to transfer an encrypted message or signature?
3. Space requirements: How many bits are required to store the key pairs and associated system parameters?

Additionally, we have considered license cost on the use of the algorithms, if any.

The key results of this study show that:

- Elliptic curve cryptosystems can provide security equivalent to RSA, but with shorter key lengths. For instance, a 3072 bit RSA key, which should be regarded as secure for at least ten years [28], is equivalent to a 256 bit ECC key. An even more long-term 512 bit ECC key is equivalent to a 15360 bit RSA key.
- ECC needs to store information about the used elliptic curve as part of the public key/certificate. This information is known as a system parameter, but is the same for all key pairs.
- RSA does have advantages when it comes to speed of encryption and signature verification, but ECC clearly outperforms RSA when it comes to decryption and signing.
- It is worth noting that ECC is much faster than RSA for key pair generation.

Furthermore, recommendations of NSA stated that [29]:
"*Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.*"

In 2015, NSA removed their recommendation to use ECC and announced that they would be moving to quantum resistant cryptography. NSA has not released any reasoning for moving away from the Suite B program (which includes ECC), other than reducing modernization costs in the near term. The NSA further states that they know neither if or when quantum computers of sufficient size to pose a threat to today's public key cryptography will be available. Furthermore, since it will be at least 5- 10 years [30] before quantum resistant cryptography is proven and standardised, we have chosen to design the PKI in a way that enables migrating to future quantum resistant cryptography without excessive costs or effort.

Table 9 outlines the perceived acceptable key lengths as of 2016.

Table 9 Comparing different key lengths with applicable validity based on [12]

Acceptable usage		RSA	ECC
Through 2030	**2031 and beyond**		
Applying Processing	Processing (legacy)	2048	224-255
Applying Processing	Applying Processing	3072	256-383
Applying Processing	Applying Processing	7680	384-511
Applying Processing	Applying Processing	15360	512+

G Certificate Loading on Ships

X.509 certificates need to be available for ships to e.g. verify signatures and encrypt messages. Only ships are discussed here, since any shore based entity will have easy access to obtain the certificates from the certificate server using a regular internet connection. There are multiple options for how to provide the certificates to the ships in due time:

1. The X.509 certificates could be embedded in every message that a ship sends or receives
2. Certificates could be downloaded by means of satellite connection when needed
3. Certificates could be exchanged between communicating parties at the start of an interaction
4. All certificates could be loaded onto the ship when in port

Alternative 1 would add approximately 1 KB of overhead to every message sent. For VDES, this would mean that 20 % of all the traffic would be X.509 certificates, if we assume a message package is 5 KB (including certificate and signature).

Alternative 2 would require every ship to have an operational satellite connection and be willing to pay the data cost of downloading certificates at relevant times.

Alternative 3 would have a worst case situation similar to alternative 1, but probably have a lower common case. However, it would need to fall back on the behaviour of alternative 1 when doing broadcasts or where it is important that not only a specific recipient verifies the information, but all the nearby ships. Optionally, the entities could regularly broadcast their certificate, but then the ships would have to store those, and it would occupy capacity on the VDES band.

Alternative 4 would require the ships to have network connectivity when in port. The first download would be in the order of 100s of megabytes, as can be seen in Figure 15, but the size of subsequent downloads would be lower (determined by the amount of new X.509 certificates since the last download). The downside is that the X.509 certificates on each ship might be out of date since the ships are in port only so often. However, given that the Certificate Revocation List (CRL) is to mainly be updated when in port, it might be sufficient that the certificates are also.

The above alternatives can be combined to create a desirable solution. E.g. could X.509 certificates be cached on ships when in port, but certificates missing from the store could be obtained by either using the satellite connection from alternative 2 or by exchanging with the other party as in alternative 3.

Configuration	Value	Unit	Lifetime	# of certificates
Certificate size	1	KB		
Trusted international CA	1	pcs	20	2
Issuing National CAs	171	pcs	10	2
Shipping companies	20 000	pcs	3	2
Vessels	125000	pcs	3	3
Ports	110000	pcs	3	3
Cache all certificates on the vessel	**Value**	**Unit**	**Yearly**	**Per port call**
Trusted international CA	2	KB	0,1	
Issuing National CAs	342	KB	34,2	
Shipping companies	40000	KB	13333,3	
Vessels	375000	KB	125000,0	
Ports	330000	KB	110000,0	
Total	745344	KB	248367,6	
	727,9	MB	242,5	14,0
Cache all shore certificates on the vessel	**Value**	**Unit**	**Yearly**	**Per port call**
Trusted international CA	2	KB	0,1	
Issuing National CAs	342	KB	34,2	
Shipping companies	40000	KB	13333,3	
Vessels	0	KB	0,0	
Ports	330000	KB	110000,0	
Total	370344	KB	123367,6	
	361,7	MB	120,5	7,0
Cache all communicating party certificates on the vessel	**Value**	**Unit**	**Yearly**	**Per port call**
Trusted international CA	2	KB	0,1	
Issuing National CAs	342	KB	34,2	
Shipping companies	0	KB	0,0	
Vessels	375000	KB	125000,0	
Ports	330000	KB	110000,0	
Total	705344	KB	235034,3	
	688,8	MB	229,5	13,2
Cache PKI Hierarchy and ports	**Value**	**Unit**	**Yearly**	**Per port call**
Trusted international CA	2	KB	0,1	
Issuing National CAs	342	KB	34,2	
Shipping companies	0	KB	0,0	
Vessels	0	KB	0,0	
Ports	330000	KB	110000,0	
Total	330344	KB	110034,3	
	322,6	MB	107,5	6,2

Figure 15 Estimations on the amount of data to cache depending on which types of certificates are stored

H The PKI solution applied to a complex scenario

To ensure that the suggested PKI for the maritime domain reflects and embraces the complexity of real-life ship operations, we have created a fictitious scenario, which represents this complexity. In this appendix we explain the role of the PKI solution in this scenario, representing an acid-test for its suitability.

The operation of a ship entails a certain set of roles. The same organisation may represent several of these roles (such as an integrated shipping company) or represent a specific role (such as a 3rd party ship manager). In addition, a ship is required to be registered to a flag state. The different roles attached to a ship will change over time as the ship is sold, is taken on by a new charterer, changes management or in some cases registered to a different flag state. This represents certain dynamics, which must be supported by the suggested PKI solution.

In the scenario, the ship "MS CySiMS" is owned by the Norwegian company "SO Norway". The ship is registered under the Bahamas Flag. "EzzonCell" (US) is the charterer. "ShipMan" (DE) is the ship manager but its daughter company "ShipManCy" (CY) holds the Document of Compliance (i.e. the document needed to manage the ship). The ship master (captain) is Polish, employed by crew manager, "CrewMan" (PL). The following actions are typically done through the voyage(s):

Table 10 Actions in a fictitious voyage and the corresponding PKI support

Action	PKI support
During the voyage, the ship passes through a ship reporting area operated by a coastal state other than the port state the ship is destined for. A report from the ship is required when entering and leaving the reporting area.	The reports will be signed by the ship X.509 certificate as described in Section 4.3.1. In case an additional signature from the master/captain is required, the report can also be signed by the master/captain's individual X.509 certificate. Encryption of sensitive information, such as crew lists and ship store inventories, can be done as described in in Section 4.3.2 or 4.3.3.
The master must send the ship's cargo declaration and other arrival documents to the port state authorities before arrival. This will in most cases be through the ship agent, but the ship will in all cases send updated crew lists and ship stores inventory itself to the port state authorities at specified time before arrival.	
In port, the ship receives new voyage instructions from the charterer. These will have to be checked and acknowledged by the captain.	
The port state (through a port state control inspection) needs access to the ship's certificates.	Accessing ship certificates does not require the support of the PKI solution. Once the port state has accessed the certificate, they can verify the authenticity and integrity of the document by using the PKI.
The ECDIS needs updated charts through the ship owner's contract with the provider of nautical information (NO). This happens on a regular basis (typically once a week) throughout the journey.	The nautical information service provider uses its service X.509 certificate to sign the update as described in Section 4.3.1. If the provider wishes to encrypt the update, it can be done as described in Section 4.3.2 or 4.3.3.

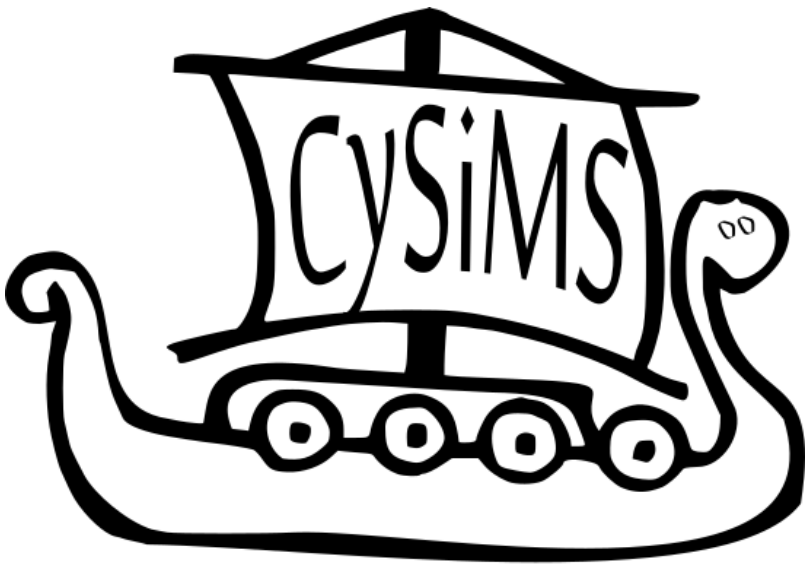
Action	PKI support
At port, the master takes his leave and is replaced with a new master, this time from Kroatia. The new master has to do or oversee all operations listed above for the new voyage.	The new master's individual X.509 certificate (crew certificate) needs to be used during the leave. Letting each master carrying his own cryptographic credentials in e.g. a removable smartcard will ensure that the correct signatures are generated in the operations listen above.
At a later point in time, the charter party expires and a new charterer "GermaChart" (DE) takes over the ship.	Unless maybe for bareboat charter[29], it will not have any impact on the PKI solution. If it is bareboat charter, it can be handled similarly to when ships are sold. The current ship X.509 certificate will be revoked in accordance to the procedure described in Section 4.5 and a new X.509 certificate for the ship with the charterer as the relevant organisation will be generated. The new X.509 certificate can be either be generated by triggering the rekeying process described in Section 4.4.2, or one can replace the smartcard in the PKI Unit and re-enrol the skip as described in Section 4.1.3.
This charterer wants to hire a new ship manager "SiShipMan" (SG) utilizing a crew manager from the Philippines called "FiCrewMan". The master (and all officers and ratings) are now Filipinos.	Letting each crew member carrying his own cryptographic credentials in e.g. a removable smartcard will ensure that the correct signatures are generated in the operations listen above.
The nautical information provider is also replaced with a German provider.	The X.509 certificate of the German service provider is already in the cache on the ship (c.f. Section 4.2), thus everything should work out of the box.
Finally, the ship is sold to a new ship owner, "DKShip" (DK). The ship owner wants to register its ship under a Danish flag. The ship owner is an integrated shipping company, which has internal ship management and commercial operations (no charterer or manager needed).	Revoke the current ship X.509 certificate in accordance with Section 4.5 and generate a new X.509 certificate for the ship with "DKShip" as the organisation. The new X.509 certificate can either be generated by triggering the rekeying process described in Section 4.4.2, or one can replace the smartcard in the PKI Unit and re-enrol the skip as described in Section 4.1.3. Note that the new X.509 certificate should be signed by the Danish Issuing National CA.
The ship is given a new name and new MMSI (as it is now registered in Denmark), but of course keeps it IMO number.	
The ship's classification company (NO) needs to issue new class certificates. This may also entail an inspection from a class society inspector.	The classification company signs the relevant documents with their private key as described in Section 4.3.4. Additional measures might be implemented on top of the PKI solution to allow for examination of documents after a rekeying of the classification company.
The ship is now classed by a German classification society. New class certificates need to be issued after transfer of class.	

Ships can be owned by organisations in one country and still be registered on the flag of another. Table 11 shows how a Norwegian company can own a ship, while it is still registered under the flag of the Bahamas.

[29] Chartering a ship without crew or provisions

Table 11 Subject X.500 Names for a ship and its owner

Entity	Entity Type	Subject X.500 Name		
		Common Name	**Organization**	**Country**
SO Norway	Organisation	SO Norway	NO123456789;SO Norway	NO
MS CySiMS	Ship	278111222	NO123456789;SO Norway	BS


CySiMS