

N/A- Unrestricted

# Report

## D2.1 Digital signatures for nautical use

### Author(s)

Karin Bernsmed, Christian Frøystad, Per Håkon Meland



# Report

## D2.1 Digital signatures for nautical use

Enterprise /VAT No:  
NO 948 007 029 MVA

**"KEYWORDS:**

PKI, maritime, security

**VERSION**

1.0

**DATE**

2016-10-27

**AUTHOR(S)**

Karin Bernsmed, Christian Frøystad, Per Håkon Meland

**CLIENT(S)**

The Research Council of Norway

**CLIENT'S REF.**

256508 /O80

**PROJECT NO.**

102013239

**NUMBER OF PAGES/APPENDICES:**

66

**ABSTRACT**

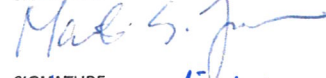
The CySiMS project aims to develop new security solutions that will provide integrated and cost-effective protection against cyber-attacks on critical safety and operational information in the maritime domain. This document outlines a Public Key Infrastructure (PKI) for maritime communication, which can be used to secure ship-to-ship, ship-to-shore and shore-to-ship communication, and discusses a number of potential deployment alternatives. 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. For the PKI solution to be adopted worldwide, it needs to be standardized.

**PREPARED BY**

Karin Bernsmed

**SIGNATURE****CHECKED BY**

Martin Gilje Jaatun

**SIGNATURE****APPROVED BY**

Arne Mikkelsen

**SIGNATURE****REPORT NO.**

N/A

**ISBN**

978-82-14-06142-0

**CLASSIFICATION**

Unrestricted

**CLASSIFICATION THIS PAGE**

Unrestricted

# Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2016-05-13	Initial version with Toc
0.2	2016-09-30	First draft version ready for internal review within consortium
0.3	2016-10-19	First complete version ready for internal QA review at SINTEF
0.4	2016-10-21	First complete version ready for internal review in the CySiMS consortium
1.0	2016-10-27	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. However, the awareness of cyber threats and their potential impacts are currently very low in the maritime domain. The objective of the CySiMS project is 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, using encryption and electronic signatures. As a part of this, the project will deliver a specification for a Public Key Infrastructure (PKI), which can be used to generate and distribute cryptographic keys amongst the involved actors.

This document outlines a PKI solution, which can be used to create, store and distribute cryptographic keys amongst a wide variety of users (including vessels, shore stations, crew members and organisations) 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 we outline a number of different alternatives for the enrolment and distribution of certificates to the vessels. We also present a number of potential deployment alternatives for storing and processing private keys and root CA certificates on board the vessels. Finally, we present a number of alternative PKI hierarchies and discuss their respective advantages and disadvantages.

A key design goal of the work presented in this deliverable has been to adapt the solution to the specific characteristics of the maritime communication infrastructure, where bandwidth is limited and where vessels can be offline at sea for long periods of time. Moreover, the proposed solution must be applicable in an international environment and fit with the existing roles and responsibilities of key stakeholders, such as International Maritime Organisation (IMO), Flag States and their Recognized Organization, Port State control, Ship-owners, crew members on board the vessels, 3<sup>rd</sup> party Application Service Providers and any other entity that would need to communicate securely. We also recognise the need for the PKI solution to be cost efficient, and to be compatible with already established digital authentication solutions in related domains (S&R operations, land based transport, etc.).

# Table of contents

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	CySiMS Overview .....	7
1.2	A brief introduction to public key cryptography and PKI.....	9
1.3	Dependencies with other deliverables .....	10
1.4	Structure of this document .....	10
<b>2</b>	<b>The need for PKI in maritime communications .....</b>	<b>11</b>
2.1	Usage context .....	11
2.1.1	Constraints .....	11
2.1.2	Required security functionality for the use cases .....	13
2.1.3	Use cases and the role of the PKI .....	14
2.2	Maritime cybersecurity regulation .....	14
2.3	Design Goals.....	15
2.4	Existing PKI solutions .....	16
2.4.1	PKI solutions for the maritime domain.....	16
2.4.1.1	LRIT security.....	16
2.4.1.2	The SafeSeaNet.....	17
2.4.1.3	The IHO Data Protection Scheme .....	17
2.4.1.4	Ongoing work on digitally signed ship certificates in ISO.....	17
2.4.1.5	Ongoing work on VDES security in IALA .....	18
2.4.1.6	Ongoing work on identity management in the Maritime Cloud .....	18
2.4.2	PKI solutions for other domains .....	19
2.4.2.1	Secure web communication .....	19
2.4.2.2	Electronic passports.....	20
2.4.2.3	Satellite communication for aviation .....	21
<b>3</b>	<b>Proposed properties for maritime PKI .....</b>	<b>25</b>
3.1	Actors involved .....	25
3.2	Digital certificates .....	25
3.2.1	The X-509 certificate standard .....	25
3.2.2	Using X.509 certificates in the maritime domain .....	26
3.3	Key material and algorithms .....	28
3.4	Storage and processing units .....	29
3.4.1	Smartcards .....	29
3.4.2	HSMs.....	30
3.4.3	Software-based.....	30

3.5	Practical options for installing the PKI system on vessels .....	30
3.5.1	Use the VDES .....	30
3.5.2	Develop a dedicated PKI unit.....	30
3.5.3	Use a conventional bridge computer .....	30
3.6	Certificate Enrolment.....	31
3.6.1	Certificate enrolment using smartcard in VDES Terminal .....	32
3.6.1.1	Alternative 1 .....	32
3.6.1.2	Alternative 2 .....	32
3.6.1.3	Alternative 3 .....	33
3.6.1.4	Alternative 4 .....	34
3.6.1.5	Alternative 5 .....	35
3.6.1.6	Alternative 6 .....	36
3.6.2	Certificate enrolment using software.....	37
3.6.2.1	Alternative 7 .....	37
3.6.2.2	Alternative 8 .....	38
3.6.3	Certificate enrolment using VDES Hardware.....	39
3.6.3.1	Alternative 9 .....	39
3.6.3.2	Alternative 10 .....	40
3.6.4	Certificate enrolment using dedicated PKI unit.....	41
3.6.4.1	Alternative 11 .....	41
3.6.4.2	Alternative 12 .....	41
3.6.4.3	Alternative 13 .....	42
3.6.5	Enrolment summary .....	42
3.7	Rekeying.....	44
3.8	Certificate Revocation.....	44
3.8.1	Certificate Revocation List .....	44
3.8.2	Online Certificate Status Protocol .....	46
3.8.3	Stapled OCSP .....	47
3.8.4	Certificate Revocation summary .....	48
<b>4</b>	<b>Alternative PKI hierarchies .....</b>	<b>50</b>
4.1	Alternative 1: IMO as root CA, Flag States and Shipowners as vertical intermediate CAs .....	50
4.2	Alternative 2: ITU as root CA, IMO and ICAO as intermediate CAs .....	51
4.3	Alternative 3: IMO as root CA, Flag States as intermediate CAs .....	51
4.4	Alternative 4: IMO as root CA, Shipowners and Flag States as horizontal intermediate CAs .....	52
4.5	Alternative 5: IMO as root CA in a flat hierarchy .....	53
4.6	Alternative 6: Flag States operate their own root CAs .....	54
4.7	Certificate chain lengths and number of CRLs .....	54
<b>5</b>	<b>Evaluation of alternatives with respect to the design goals.....</b>	<b>56</b>

**6    Summary and future work.....61**

**A    Abbreviations and glossary.....64**

## 1 Introduction

The European maritime sector and infrastructure is critical to the world economy. Whereas maritime activities are relying more and more on ICT, the awareness on cyber security requirements and challenges in the maritime sector is currently low to non-existent [1].

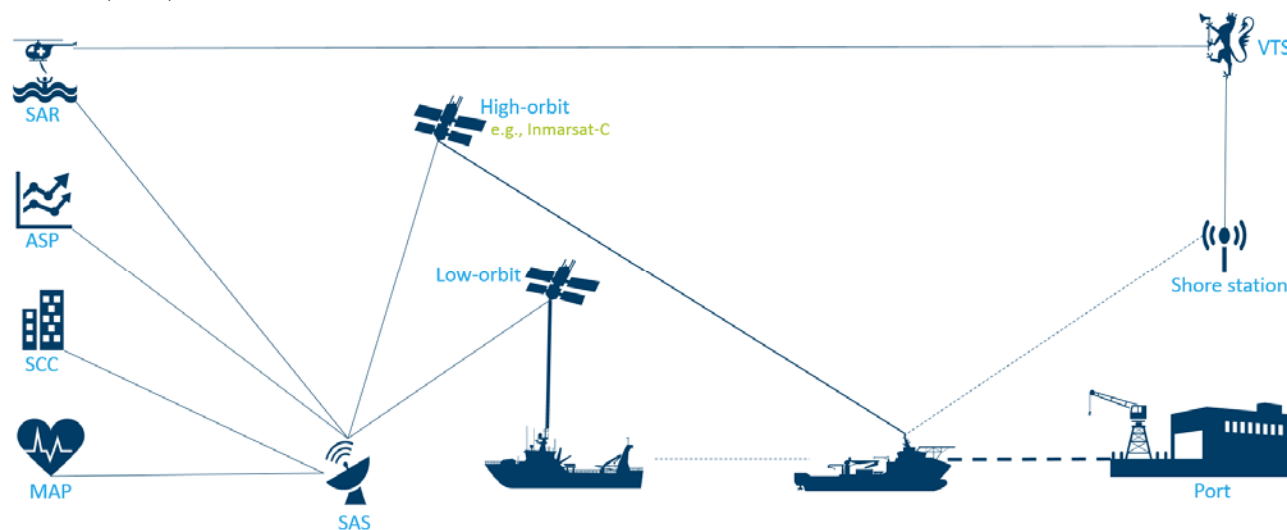
History shows that maritime terrorist attacks are real threats, e.g. Achille Lauro in 1985 [2], Limburg in 2002 [3] and Superferry 14 in 2004 [4]. All these were physical attacks on ship and passengers, but it is only a matter of time before cyber-attacks are also part of the terrorists' weapons.

The underlying idea of CySiMS is to develop new maritime security solutions that provide integrated and cost-effective protection against cyber-attacks on critical 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. Given that CySiMS mainly concerns the coming VHF Data Exchange System (VDES) technology, it also focuses mainly on the future Maritime Service Portfolio (MSP) rather than the current situation.

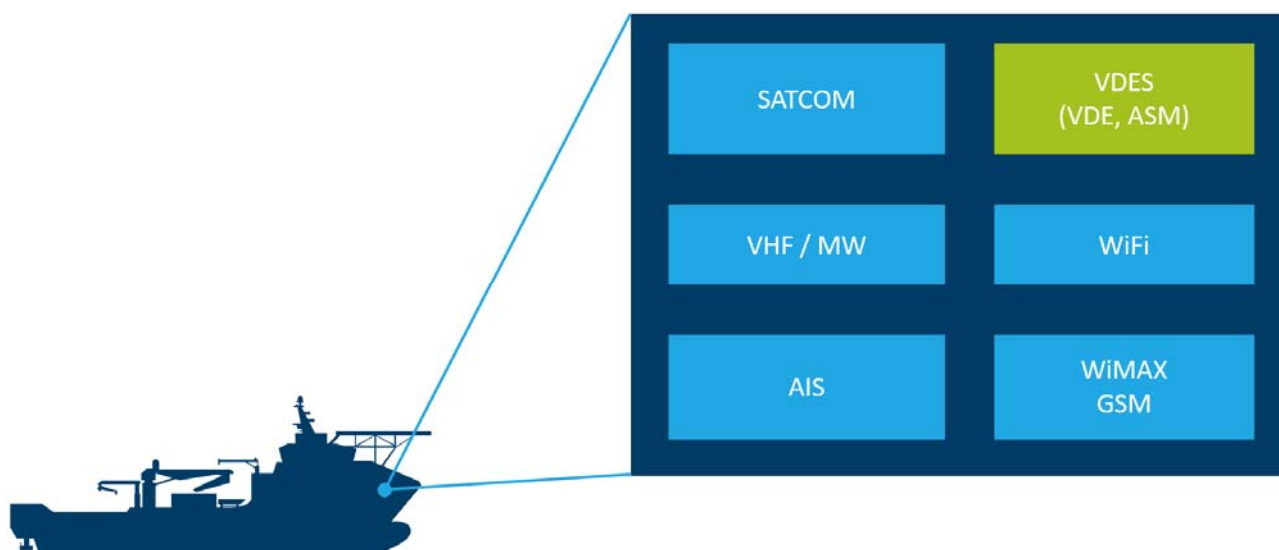
As can be seen in Figure 1, CySiMS aims to handle a diverse set of interactions including ship to ship, ship to port, ship to Shipping Coordination Centre (SCC), ship to Vessel Traffic Services (VTS), ship to Application Service Provider (ASP), ship to Medical Aid Provider (MAP), and coordination of Search and Rescue (SAR).



**Figure 1 High level overview of the CySiMS ecosystem**

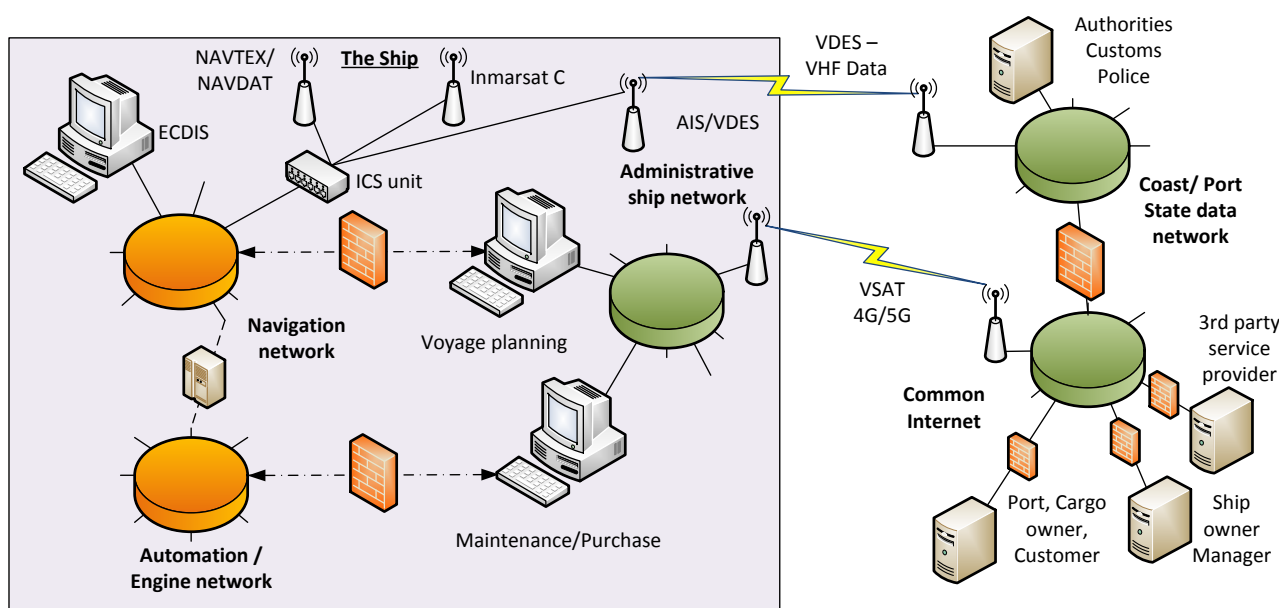
By transitioning from analogue voice over VHF radio to digital messages over the VHF Data Exchange System (VDES) and introducing more use of satellite communication (SATCOM), the stress on the current communication links are reduced and new services can be introduced. The use of the different communication links, which can be seen in Figure 2, will depend on the ship's location, information to be transmitted, and the stage of the ship's journey.





**Figure 2 Communication systems commonly found on ships. VDES, the green box, is expected to become commonly used once completed**

The CySiMS security solution will not be introduced into a vacuum, but will need to coexist with existing systems and architectures of the systems on ships. Figure 3 shows a typical ship data network topology in relation to different actors and systems. Data enters the ship through communication channels such as VDES and VSAT, and enters different subnetworks separated by firewalls.



**Figure 3 Typical ship data network topology**

The role of work package H2 in the CySiMS project is to develop an encryption and electronic signature scheme suitable for the characteristics of the maritime ecosystem. This includes defining a Public Key Infrastructure (PKI), which can be used for authentication and to establish cryptographic protection of ship-to-shore, shore-to-ship and ship-to-ship communication.

## 1.2 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 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 certificates. A PKI is defined in RFC 4949 [5] as a set of hardware, software, people, policies and procedures that are needed to create, manage, store, distribute and revoke digital 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 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 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) 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 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 certificates and CRLs so that they can be retrieved by the end entities

A **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 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.

### 1.3 Dependencies with other deliverables

This deliverable is related to the following other deliverables in the CySiMS project

- The deliverable "*D1.1a Context and user requirements*" outlines a number of high-level use cases for the maritime domain. The usage context and design goal for the PKI solution are based on these use cases.
- The deliverable "*D1.1 Risk model and analysis*" will provide a method for risk assessments in the maritime domain, relevant contextual information and building blocks like threat actors and common threats. The resulting document will have implications for the PKI solution, which will depend on the risk and threat environment in which it is supposed to operate. Results from D1.1 will be therefore be incorporated in the work with the PKI solution as needed.

This deliverable "D2.1 Digital signatures for nautical use" outlines and discusses potential alternatives for designing, implementing, deploying and operating a PKI. The results from this deliverable will serve as input to the forthcoming deliverable "D2.2 Using digital signatures in the maritime domain". While the main purpose of D2.1 is to present and analyse potential alternatives, D2.2 will focus on the usage of the selected alternatives.

### 1.4 Structure of this document

The rest of this document is structured as follows. Section 2 presents the context that the PKI solution will operate in and the requirements and design goals that we have derived for the solution. We also discuss ongoing work related to PKI in the maritime domain, and outline some existing solutions. In Section 3, we present the most important properties of the a maritime PKI solution, i.e. the use of digital certificates, the selection of algorithms and key lengths, and outline some potential certificate enrolment and revocation solutions. Further, Section 4 discusses alternative PKI hierarchy solution. Section 5 evaluates the different solutions against the stated design goals, before Section 6 concludes the documents with a summary and future work.

## 2 The need for PKI in maritime communications

This section derives requirements for the CySiMS PKI solution and outlines a set of design goals that the solution should fulfil.

### 2.1 Usage context

As was illustrated in Figure 1, CySiMS aims to handle a diverse set of interactions between ships and shore stations. To derive requirements for the PKI solution we have used a number of high level use cases (see Section 2 in the *D1.1a Context and user requirements* document [6]), which outlines how the system is intended to be used. These use cases are:

- UC1.1 Issue and store ship certificate
- UC1.2 Third party verification of ship certificates
- UC1.3 On board inspection of ship certificates
- UC1.4 Ship certificate endorsement
- UC1.5 Ship certificate revocation
- UC2.1 Successful port clearance, which includes transmitting and verifying ship certificates from the ship to the port
- UC2.2 Unsuccessful port clearance, which includes transmitting and (unsuccessfully) verifying ship certificates from the ship to the port
- UC3.1 Maritime safety information to ships, which includes broadcasting safety critical information to the ships
- UC3.2 Nautical publication service, which includes distributing information with commercial and/or operational value
- UC3.3 Traffic organisation service, which include ship-to-VTS interaction to plan an optimal route through a congested area
- UC3.4 Automatic reporting, which is similar to the Maritime Single Window<sup>1</sup> but implemented over a VDE data link
- UC3.5 Tug remote control
- UC4.1 Deck log book
- UC5.1 Nautical chart update
- UC6.1 Access information on the VDES Bulletin Board

Please refer to [6] for further details about the use cases.

#### 2.1.1 Constraints

In addition to the high-level use cases, [6] 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 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 cost and the network characteristics of the PKI solution.

**Cost.** Shipping is a low cost business and this imposes limitations on which solutions could be acceptable to the industry. The costs must be kept sufficiently low for potential users such as:

- Ship owners
- Port state authorities

---

<sup>1</sup> A Maritime Single Window is a portal where users (Ship Owners or their authorized agents) can submit necessary electronic information, such as ship pre-arrival reports. "This single window shall be the place where all information is reported once and made available to various competent authorities and other Member States"

<http://www.emsa.europa.eu/nsw.html>

- Ports
- Flag states and their recognized organisations
- Operators of any security mechanisms included in the PKI solution

**Cost types.** Costs come in multiple types and forms, and are imposed on 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.

**Network characteristics.** The communication capacity is limited and it is therefore important to include both stress on communication links and operational costs when considering the costs of a solution. Table 1 outlines the data capacity of the different communication links that will be used.

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 <sup>2</sup>	Near shore
SATCOM	1 – 8 Mbps	About 5.25 USD per MB <sup>3</sup>	Globally
WiMAX	10 - 100 Mbps	Free <sup>4</sup>	Near ports

**Table 1 Data capacity and cost of different data bearers**

Throughout this document, since the message formats and protocols for VDES is still in flux, it is assumed that a VDES message has an average payload of about 5 KB.

**Bit Error Rate.** The design must consider the bit error rate (BER) of the communication link in order to ensure that the solution will work under real circumstances. Table 2<sup>5</sup> shows the probability of a package of a given length (left column) containing at least one bit error at different BERs (first row). Since the BER of VDES is not known yet, and since we do not know how PKI solution will contribute to the package length, this table must be re-considered and revisited in deliverable D2.2, when the PKI is being designed. It is however likely that packet error rates that are less than 1% will be of little significance.

<sup>2</sup> 5 GB monthly plan at 249 NOK for use in Norway at <https://www.telenor.no/bedrift/mobilt-bredband/>

<sup>3</sup> 100 MB prepaid SIM for \$525 USD at [http://www.groundcontrol.com/BGAN\\_rate\\_plans.htm](http://www.groundcontrol.com/BGAN_rate_plans.htm)

<sup>4</sup> Provided that the port offers such capabilities and includes any required maintenance costs in their ordinary port fees

<sup>5</sup> 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 %

**Table 2 An overview over the packet error rates for different package lengths (PL) (left column) and bit error rates (BER) (first row)**

### 2.1.2 Required security functionality for the use cases

In Table 3, the high-level use cases from [6] are mapped to the security functionality that they will require.

Use Case	Authentication (entity)	Integrity protection	Confidentiality	Electronic signature generation	Electronic signature verification	Electronic signature revocation	Media	Unicast / Multicast
UC1.1	✓ (flag state authority)	✓		✓			VSAT	U
UC1.2	✓ (flag state authority, port state authority)	✓			✓		VSAT	U
UC1.3		✓			✓		e.g. WIFI	U
UC1.4		✓		✓			VSAT	U
UC1.5		✓				✓	VSAT	U
UC2.1	✓ (vessel, port state authority)	✓	✓*		✓		VSAT / VDES	U
UC2.2	✓ (vessel, port state authority)	✓	✓*		✓		VSAT / VDES	U
UC3.1	✓ (VTS, service providers)	✓					VDES VSAT	M
UC3.2	✓ (service providers)	✓	✓*				VSAT VDES	M
UC3.3	✓ (vessel, VTS)	✓					VDES	U/M
UC3.4	✓ (vessel, VTS)	✓	✓*		✓		VDES	U
UC3.5	✓ (vessel, user)	✓					VDES	U
UC4.1	✓ (user)	✓		✓			VSAT VDES	U
UC5.1	✓ (vessel, service provider)	✓	✓*				VSAT	U
UC6.1	✓ (VTS)	✓					VDES	M

**Table 3 Mapping of high-level use cases to relevant security functionality**

\* Either the content or the communication channel should be encrypted (or both).

### 2.1.3 Use cases and the role of the PKI

In Table 4, we outline how a PKI solution can be used to provide the required security functionality in Table 3.

Use Case	Support by PKI
UC1.1	The PKI can provide the cryptographic keys needed for the inspector's organisation to create a digital signature of the ship certificate, and to prevent it from being modified
UC1.2	The PKI certificates can be used to verify the ship certificate integrity, and authenticate the issuer. The PKI could also be used to authenticate the foreign port state authority that is requesting the certificate.
UC1.3	The PKI certificates can be used to verify the ship certificate integrity and authenticate the issuer
UC1.4	Similarly to UC1.1, the PKI can be used to renew the digital signature of a ship certificate and to prevent it from being modified.
UC1.5	By revoking the ship certificate issuer's PKI certificate, the digital signature on the ship certificate can be invalidated.
UC2.1	The PKI can allow the ship to authenticate itself, to sign the data to be sent and to verify the identity of the recipient. The PKI can also be used to ensure the confidentiality of the data by encrypting either the data or to establish an encrypted transportation channel. The PKI can also guarantee that the clearance, or lack thereof, is issued by the correct party
UC2.2	The PKI can allow the ship to authenticate itself, to sign the data to be sent and to verify the identity of the recipient. The PKI can also be used to ensure the confidentiality of the data by encrypting either the data or to establish an encrypted transportation channel. The PKI can also guarantee that the clearance, or lack thereof, is issued by the correct party
UC3.1	The PKI can ensure the integrity of the message and the authenticity of the sender
UC3.2	The PKI can ensure the integrity of the message, the authenticity of the sender and receiver, and can also be used to encrypt the content of the message
UC3.3	The PKI can ensure the integrity of the message and the authenticity of the sender and recipient
UC3.4	The PKI can allow the ship to authenticate itself, to sign the data to be sent and to verify the identity of the recipient. The PKI can also be used to ensure the confidentiality of the data by encrypting either the data or to establish an encrypted transportation channel. The PKI can also guarantee that the clearance, or lack thereof, is issued by the correct party
UC3.5	The PKI can ensure the integrity of the instructions and the authenticity of the sender and recipient
UC4.1	The PKI can ensure the integrity of the entries and the authenticity of the ship and person signing them
UC5.1	The PKI can ensure the integrity of the messages, the authenticity of the sender and receiver, and can also be used to encrypt the content
UC6.1	The PKI can ensure the integrity of the bulletin board and the authenticity of the issuer

**Table 4 An overview over how a PKI can support the security needs of the high-level use cases**

## 2.2 Maritime cybersecurity regulation

This chapter aims to identify whether there are any external requirements from maritime regulation that we need to consider when designing a PKI solution in the CySiMS project.

The maritime sector currently does not have any regulations on cybersecurity, however, this is about to change. The IMO Maritime Safety Committee has recently formed a working group on security, which has published a document on guidelines for cybersecurity on board ships [7]. Here we cite some of the key considerations from this document, which regard technical security controls relevant to the communication equipment and software systems onboard ships.

Regarding the satellite and radio communication link, the guideline document states that

*"Cybersecurity of the radio and satellite connection should be considered in collaboration with the service provider. In this connection, the specification of the*



*satellite link should be taken into account when establishing the requirements for onboard network protection"*

and

*"When establishing an uplink connection for ships' navigation and control systems to shorebased service providers, it should be considered how to prevent illegitimate connections gaining access to the onboard systems"*

Regarding application software security and patch management, the document further states that

*"Critical safety and security updates should be provided to onboard systems. Such updates or patches should be applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a cyber attack"*

These are the only parts of the guideline that are relevant for the design of the PKI solution. None of these recommendations will impose any requirements on our work, however, we can conclude that a PKI solution can help meet these recommendations by 1) ensuring mutual authentication of the end-points utilizing the satellite and radio communication links, and 2) providing a secure channel for distributing critical software updates to the onboard ship systems.

In addition to the IMO guidelines, there is ongoing work in *ISO/TC8 Ships and marine technology* on the potential standardization of digitally signed ship certificates (see [8]). The ISO/TC8 work will be further described in Section 2.4.1.4; however, we note that the design of the CySiMS PKI solution should be compatible with the ISO proposal, in case their solution will be standardized.

Finally, the IALA ENAV Committee WG3 Telecommunications is currently considering a proposal on integrity monitoring and authentication for VDES through the use of pre-distributed public keys [9] (this solution will be further described in Section 2.4.1.5), which is intended to be integrated as an annex in the draft IALA guideline on VDES. The proposal is only an early draft, but we will monitor its progress closely during the course of the CySiMS project.

## 2.3 Design Goals

This subsection outlines the design goals for the CySiMS PKI solution. The design goals have been derived from the usage context and security needs identified in Section 2.1 and 2.2, from the use case descriptions in [6] and from internal discussions within the CySiMS consortium. The following goals have been identified:

- 1) **Identification and authentication.** The PKI solution should support identification and authentication of a large number of end entities, consisting of a wide variety of vessels, shore stations, individual users, organisations and application services
- 2) **General applicability.** The PKI solution should be made available for all vessel systems that require cryptographic protection
- 3) **Digital signatures.** The PKI solution should support digital signatures of application data, e.g. electronic ship certificates and log book entries
- 4) **Offline cryptographic verification.** The cryptographic properties of the PKI solution (digital signatures etc.) must be verifiable offline – ships and inspectors are not always online
- 5) **Future service applicability.** The PKI solution should be extendable to support the security needs of future maritime services.
- 6) **Low bandwidth needs.** The PKI solution must be suitable for the maritime communication infrastructure where bandwidth is limited



- 7) **International applicability.** The PKI solution must be applicable in an international environment and fit with the existing roles, responsibilities and trust relationships of the involved stakeholders (IMO, flag states, coastal states, shipowners etc.).
- 8) **Compatible.** The PKI solution should be compatible with already established PKI hierarchies in related domains (Search and Rescue operations, land based transport, etc.)
- 9) **Low cost.** The costs of the PKI solution should be minimized
- 10) **Long-term risk.** The security strength of the PKI solution should be based on a long-term risk analysis, where future threats are identified and evaluated.
- 11) **Compliance.** The PKI solution must be compliant with applicable legislations, regulations and standards worldwide.
- 12) **Global deployment and operation.** The deployment and operation of the PKI infrastructure, including enrolment, distribution and revocation of ship certificates, must be manageable in a global environment.
- 13) **Key management.** The PKI solution should include secure generation, storage and processing of private keys and root certificates.
- 14) **Cryptographic migration.** The PKI solution should enable migration to future cryptographic solutions without excessive costs or efforts

## 2.4 Existing PKI solutions

A number of PKI solutions already exist, both for maritime purposes as well as in other domains. In this subsection we outline some of these, discuss lessons learnt related to the work presented in this deliverable and evaluate their potential applicability to CySiMS.

### 2.4.1 PKI solutions for the maritime domain

There exist several PKI solutions in the maritime domain at different scales and for different purposes.

#### 2.4.1.1 LRIT security

The long-range identification and tracking (LRIT) system [10] [11] 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) [12] 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.

#### 2.4.1.2 The SafeSeaNet

The SafeSeaNet (SSN) is a vessel traffic monitoring and information system operated by EMSA<sup>6</sup>. 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 [13].

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.

#### 2.4.1.3 The IHO Data Protection Scheme

International Hydrographic Organization (IHO) S-63 [14] 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 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.

#### 2.4.1.4 Ongoing work on digitally signed ship certificates in ISO

ISO/TC 8 Ships and marine technology has investigated how digitally signed ship certificates<sup>7</sup> can be standardized in the maritime domain, and propose to use a PKI to implement this [8]. 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

---

<sup>6</sup> <http://www.emsa.europa.eu/ssn-main.html>

<sup>7</sup> "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.

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 [8], 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<sup>8</sup>, 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.

#### **2.4.1.5 Ongoing work on VDES security in IALA**

A recent working document from an IALA committee [9] 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. 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.

#### **2.4.1.6 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<sup>9</sup> where organisations can log in, create an X.509 certificate signing request, which will then

<sup>8</sup> Global Integrated Shipping Information System. <https://gisis.imo.org/Public/Default.aspx>

<sup>9</sup> <http://developers.maritimecloud.net/identity/index.html>

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<sup>10</sup> [15][16].

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.

## 2.4.2 PKI solutions for other domains

The PKI concept has also been deployed in numerous other settings than the maritime domain. Here we describe three examples of existing PKI applications with some "lessons learned" that are relevant for the CySiMS project. The purpose of this section is to illustrate how some of the challenges one will experience when designing a PKI solution have been solved in other domains.

The three examples are

- Secure web communication, where PKI is used to authenticate web servers and clients and to provide transport layer security (HTTPS) through the use of TLS/SSL
- Electronic passports, where PKI is used to make it easier to verify the authenticity of passports, and
- Satellite communication for aviation, where PKI is used to authenticate aircraft and ground stations and provide network layer security through the use of IPsec

### 2.4.2.1 Secure web communication

The most common application of PKI today is to secure web communication. TLS (the successor of SSL) is the most widely recognised protocol used to provide secure HTTP (HTTPS) connections between web browsers and web servers over the Internet. TLS uses X.509 certificates to authenticate web servers and to set up an encrypted and integrity protected communication link between the client and the server. TLS also supports client (end user) authentication by the use of certificates, even though this option is rarely used.

To obtain an X.509 certificate for a TLS server, one can either purchase a certificate from an established Certificate Authority (CA), such as Symantec<sup>11</sup>, or create a self-signed web certificate. The CA certificates that are trusted by the browser are defined in its "root certificate store", which has been pre-installed by the manufacturer of the client-machine. When a user connects to a website over HTTPS, the web server presents a certificate that may be signed by another certificate, which may be signed by another certificate, until one reaches one of the CA certificates in the browser's root store. The browser will display a warning to the user in case the chain of certificates reaches a root CA that is not trusted by the browser, or if the web server uses a self-signed certificate.

---

<sup>10</sup> <http://efficiensea2.org/>

<sup>11</sup> <https://www.symantec.com/ssl-certificates/>

When surfing the Internet over HTTPS, the browser is responsible for checking the revocation status of the web server certificate for the web site that the user visits, and this is done either by regularly retrieving CRLs from the CAs in the browser's root certificate store, or by using an online certificate status protocol to gather real-time revocation information from the CAs.

Highlights from secure web communication:

- ➔ Server authentication over HTTPS is the most common use case
- ➔ The PKI infrastructure is well established; internationally trusted root CA certificates are pre-installed in most web browsers
- ➔ Self-signed and expired web server certificates are common problems; users therefore tend to ignore and override the browser warnings of certificate problems

Applicability to CySiMS: None, but the secure web communication example demonstrates that PKI is a viable solution for application layer security on an inherently untrusted network and that it can be successfully implemented for worldwide use with a very large number of end entities.

#### 2.4.2.2 Electronic passports

Electronic passports (e-Passports) [17] [18] have been used in the European Union since 2006. The main objectives of e-passports are to strengthen the link between the passport and its user, and to make it easier to verify the authenticity of the passport.

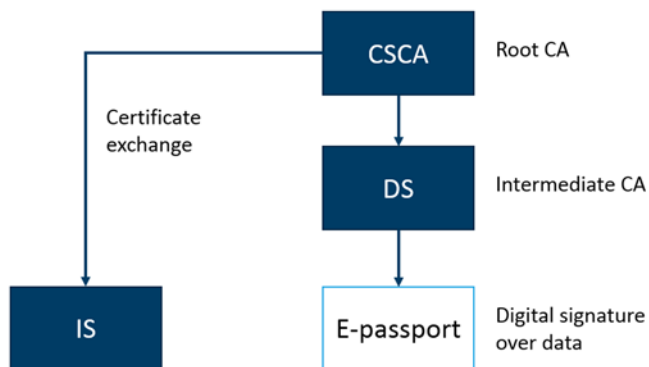
E-passports issued after June 2009 include a short-range proximity radio-frequency chip that contains a digital facial image and two digital fingerprints. The chip also includes an electronic signature over the biometric data, as well as the certificate of the entity that has created the signature. The e-passport is presented at border control, where an Inspection System (IS) will read the biometric content of the chip to determine whether the passport is genuine, valid and belongs to the bearer.

E-passports, formally denoted electronic Machine Readable Travel Documents (e-MRTDs), use two different PKIs: one to sign the passport data and another to verify the signature<sup>12</sup>.

The "signing PKI" is used to verify the integrity and authenticity of the data in the e-MRTD chip. The signing PKI consists of a Country Signing Certification Authority (CSCA) and one or more Document Signers (DS). The DS keys are used for a limited amount of time, usually three months, and sometimes also for a limited number of passports. To verify the data in e-MRTDs from foreign countries, a national Inspection System can obtain DS certificates for the other countries from a Public Key Directory operated by ICAO, via diplomatic channels or via the so called "master lists". The signing PKI is illustrated in Figure 4.

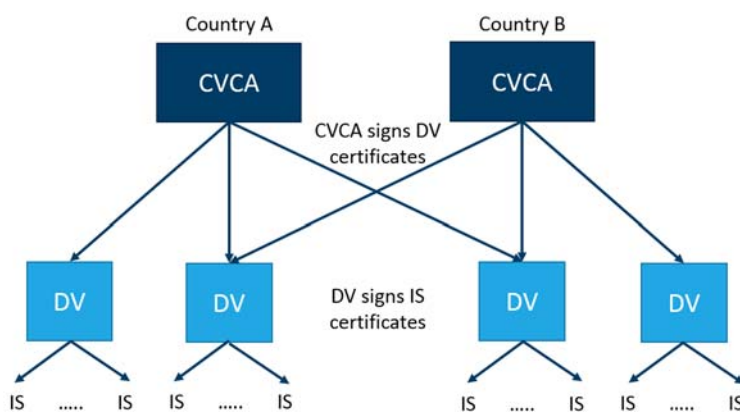
---

<sup>12</sup> In addition a third PKI for securing the exchange of certificates between different countries has been proposed, but, as far as we are aware, this has not yet been widely adopted.



**Figure 4 E-passports: Signing PKI hierarchy**

The "verification PKI" enables the e-MRTD chip to verify the authenticity of the Inspection System (IS) in order to control the access to the biometric data stored in the chip. The verification PKI consists of a Country Verifying Certification Authority (CVCA), one or more Document Verifier Certification Authorities (DVCA) and the IS. The verification PKI is illustrated in Figure 5.



**Figure 5 E-passports: Verification PKI hierarchy**

Highlights from e-passports:

- ➔ E-passports has adopted a distributed trust model, in order to avoid having to trust a single root CA. Country-specific PKIs are used; one for signing and another one for verification.
- ➔ The key distribution problem is solved by offering two different means to access root certificates from foreign countries; through bilateral means (diplomatic channels) or through an electronic exchange (ICAO Public Key Directory or "master lists").
- ➔ E-passports use Card verifiable certificates (CVC) [17], which are digital certificates that are designed to be processed by devices with limited computing power.

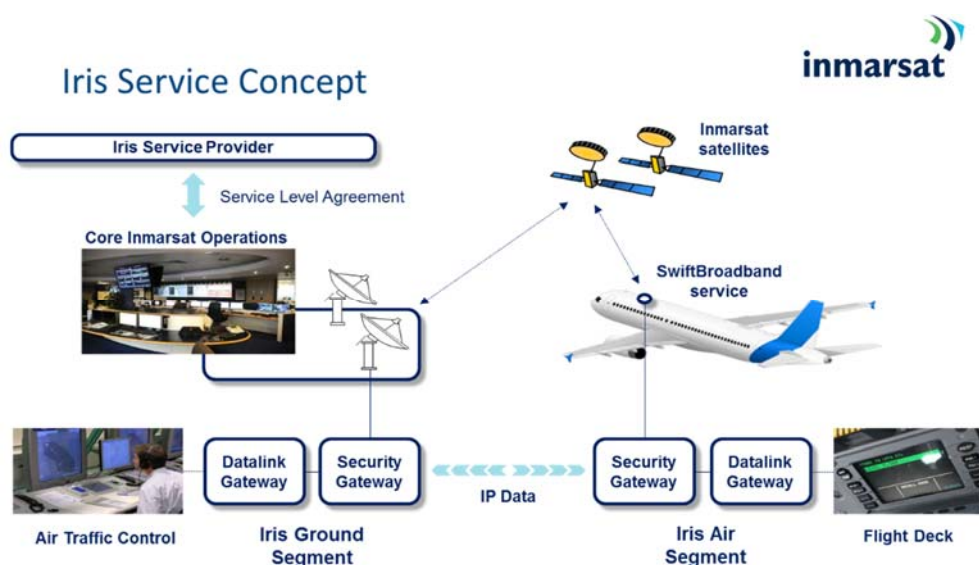
Applicability to CySiMS: None, but the distributed trust model is interesting for the maritime domain where not all the Flag States will be equally trusted.

### 2.4.2.3 Satellite communication for aviation

The European Union is implementing a series of administrative, operational and technical enhancements to European Air Traffic Management (ATM) through the Single European Sky ATM Research (SESAR) programme. In order to increase the data communication capacity and support new flight management concepts such as 4D trajectory management, the European Space Agency's Iris Precursor programme has been established to provide a SATCOM data link service in the 2017-2025 timeframe. The aviation

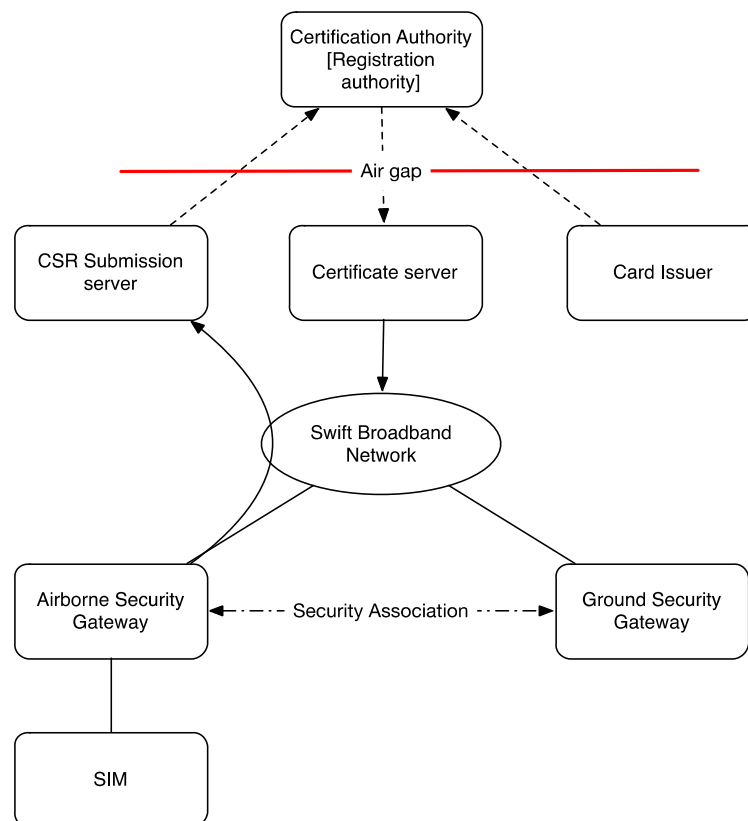


communications service is based on the existing Inmarsat SwiftBroadband (SBB) service. This would augment existing VHF Datalink (VDL) capability in Europe to improve current Link2000+ and planned I4D ATS datalink service [19].



**Figure 6. Aviation: The Iris service concept (figure by Inmarsat)**

A central component of Iris Precursor is the development of a PKI that ensures that all communicating entities can authenticate each other in a secure and reliable way, and that a secure network (IPsec) can be set up between these entities. To this end, the PKI provides a central trusted certificate authority to issue certificates binding the private key of the entity to its identity. Hence, peers can safely assume that an entity holding the private key corresponding to the public key found in a certificate is authentic.



**Figure 7: Aviation: PKI and relation to air and ground security gateway**

In order to provide such assurance, the PKI subsystem is divided into four components.

- The Certificate Authority (CA) - is an offline entity operated in a secure and trustworthy environment providing the root of trust of the PKI. Any public key and identity signed by the CA will be trusted to be accurate by the other entities in the system.
- The Registration Authority (RA) is a software component operating offline in a secure and trustworthy environment ensuring that registration information provided in the enrolment process is genuine and accurate.
- The Certificate Server – is an online entity responsible for delivering certificates and certificate revocation lists (CRLs) on request to any entity in the system.
- The CSR Submission server – is an online entity, facilitating reception of Certificate Signing Requests (CSR) to the CA.

These components and their relations are shown in Figure 7. In the figure, dashed lines are used for logical connections (not online) and fixed lines are used for network connections (online). In addition to these components, the Ground Security Gateway (GSGW) and Airside Security Gateway (ASGW) will store the PKI certificates for communicating securely with each other. There is a smart card used for this purpose in the ASGW, which must be initialized on the ground before it is installed in the Airborne Security Gateway. The main criterion is that initialisation is done in a trusted zone in order to establish the Security Association, for instance at the manufacturer site or at the premises of Inmarsat.

Highlights from Iris Precursor PKI:

- ➔ Though components are designed to be long-lasting (10-20 years), we must assume that they will break at some point of time, and aviation has strict time constraints on how long an aircraft can be grounded before a replacement part should be installed. For a PKI solution, this includes not only



physical components such as smart cards, but also a new enrolment of PKI certificate. Any solution must be optimized for quick replacement anywhere in the world.

- ➔ Any instalment or replacement should not require advanced technical knowledge by mechanics. Mechanisms such as activation codes/activation servers for smart cards were regarded as too complex.
- ➔ There are many actors involved (airlines, airports, crew, mechanics, operators, manufacturers, etc). Assume that only a very small selection of these can be fully trusted, and the rest must be able to operate without this trust. Ensure that information critical to the PKI solution (certificates, certificate signing requests, certificate revocation lists) are self-protected and can be sent over open/insecure channels.
- ➔ Pre-loading smart cards with independent private keys and exporting corresponding public keys to the CA before deployment allows for less critical message exchange during a re-key process. By putting more trust in such a hardware secured module, the overall attack surface is reduced.

Applicability to CySiMS: The aviation and the maritime domains have many similar characteristics and we should look into the Iris Precursor PKI solution when looking for solutions to the challenges we will encounter. In particular, many of the issues related to limited bandwidth and to enrolment and revocation of certificates for entities that are offline, have already been solved in the Iris Precursor solution.

### 3 Proposed properties for maritime PKI

This section provides our proposed properties for the PKI solution, in terms of 1) the actors involved in the operation and usage of the PKI, 2) what standard we recommend for the digital certificates and how they should be formatted, 3) our recommendations for key material and algorithm, and 4) different options for enrolment and revocation of the digital certificates to the end entities.

Please note that for some of the properties we have already made a decision on what is the best solution, while for others we outline potential options and discuss their pros and cons without making any recommendation. As stated in the introduction, the main purpose of this deliverable (D2.1) is to present and analyse potential alternatives; our next deliverable (D2.2) will focus on the usage of the selected alternative.

#### 3.1 Actors involved

The following actors might be involved in the proposed PKI solution:

- A **trusted international organisation** is needed, which will serve as the root of trust in the PKI hierarchy and which will operate the root Certificate Authority (CA). This role could be taken by IMO, which is already operating the root CA for the LRIT system<sup>13</sup>. Other potential candidates for operating the root CA are IALA, EMSA or IHO. There might be a need for the trusted international organisation to operate on some flag states' behalf due to lack of resources or competence.
- The **Flag States (FS)**, or any of their associated **Recognised Organisations (RO)**
- The **Vessel Traffic Service (VTS)**, which is the marine traffic monitoring system that has been established by a coastal state.
- The **shipowners** are organisations that own ships, potentially under different flags
- The **vessels** are any boats or ships that need the communication and information solutions relied upon in the use cases mentioned in section 2.1
- The **agents** are the organisations that represents the shipping company in foreign port
- The **Application Service Providers (ASPs)** are organisations providing services to shipping companies and vessels
- The **crew** members are users who use the communication and computer systems

#### 3.2 Digital certificates

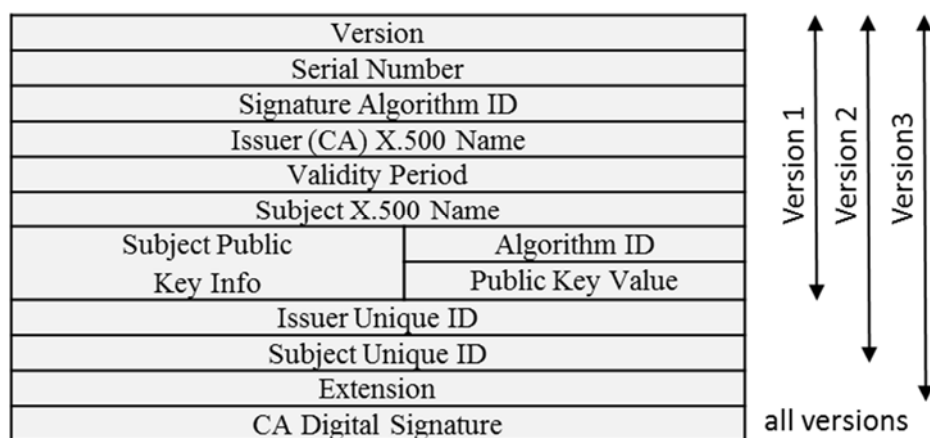
As explained in Section 1.2, a PKI uses a digital certificate to bind a public key of an entity to that particular entity. To choose a digital certificate standard for the purpose of maritime communication, we need to consider the feasibility, cost and bandwidth required for implementing, deploying and operating the standard.

##### 3.2.1 The X-509 certificate standard

The most commonly used certificate standard for PKI is X.509 [20], [21], which is commonly used for deploying certificate-based architectures on the Internet. The structure of an X.509 certificate is shown in Figure 8. The most interesting elements of the certificate are the **Issuer CA X.500 Name**, which includes the name of the CA that has signed the certificate, the **Validity Period**, which contains two dates: the first and last on which the certificate is valid, the **Subject X.500 Name**, which contains the name of the entity that the certificate refers to, the **Public Key Value**, which contains the public key that belongs to the entity and the **CA Digital Signature**, which contains a hash code of all the other fields in the certificate that has been encrypted (signed) by the issuing CA's private key. In addition, the X.509 v3 **Extension Field** permits any number of additional fields to be added to the certificate. Certificate extensions provide a way of adding information, for example usage restrictions of the certificates. Note that the fields "Issuer Unique ID", "Subject Unique ID" and "Extension" are optional in X.509 v3.

---

<sup>13</sup> IMO has also been proposed by ISO to act as the root of trust in a PKI for digital signatures of ship certificates [8].



**Figure 8 The structure of an X.509 certificate**

The size of an X.509 certificate will vary, depending on which version is used, what format the certificate is stored in, which extensions are being applied (if version 3 is used) and what key type and key size is used for the key pair. As an example, a rough estimate of the size of an X.509 v1 certificate in DER format with a 8192 bit RSA public key is 1500 bytes<sup>14</sup>.

X.509 is by far the most well-known and well-adopted standard for digital certificates, however, another alternative exist. Card Verifiable Certificates (CVC) [17], which are used in European ePassports (see Section 2.4.2.2), has been specifically designed to be processed by devices with limited computing power. CVC use fixed fields for information encoding, which means that parsing of the certificate will require less processing power and memory consumption. This could be important if the certificates are to be stored and processed in smartcards or similar elements. Even though parsing will be simplified, the size of a CVC certificate will not be noticeably smaller than the size of an X.509 certificate, since the entity's public key, and the CA's digital signature of the certificate, will take up most of the space in the certificate anyway. Also, since X.509 is the dominating standard, it will most likely be both easier and cheaper to acquire open source or COTS software for deploying the PKI solution. In our opinion, to meet the design goals on limiting the required bandwidth and minimizing the operational costs, there are other issues, for example, how to enroll and manage the certificates (see Section 3.6-3.8) and what PKI hierarchy to use (see Section 4), which are of more concern than what certificate standard to use. Our recommendation in the CySiMS project is therefore to utilize the X.509 v3 standard for digital certificates for the maritime domain.

Note that X.509 v3 is the latest version of the X.509 standard and, as illustrated in Figure 8, it contains an extension field that was not part of v1 and v2. This field will increase the certificate size, but since it is optional, it should only be used if needed. This issue will be discussed in the next subsection.

### 3.2.2 Using X.509 certificates in the maritime domain

Having identified X.509 as an appropriate standard, we need to consider how the standard can be used. Recall the structure of an X.509 v3 certificate in Figure 8. Most of the fields (e.g. Version, Serial number, Signature Algorithm ID, etc.) will be generated automatically for each certificate request. However, some fields need to be carefully chosen in order to fit the context of maritime communication. These are:

- Subject X.500 name

<sup>14</sup> See <http://fm4dd.com/openssl/certexamples.htm> for a collection of X.509 certificates with varying key types and sizes

- Issuer (CA) X.500 name
- Issuer unique ID
- Subject unique ID
- Extension
- Validity period
- Signature Algorithm ID, Subject Public Key Info and Algorithm ID

As mentioned in Section 2.4.1.6, the Maritime Cloud Identity Platform has already implemented a prototype web-based portal where organisations can register and log in to request the Maritime Cloud CA to issue X.509 v3 certificates for their vessels. The proposed formatting of the fields in the X.509 v3 certificates in this document is similar, but not identical, to their approach<sup>15</sup>.

The **Subject X.500 Name** field will be used to identify the owner of the public key in the certificate. As outlined in Table 5, we propose the field to consist of the following information, dependent on whether the owner of the certificate is a vessel, a service, a (human) user or an organisation:

- The Common Name (CN) will be used to display the name of the entity. 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 Organizational Unit (OU) will be used to indicate what department / group /section the entity belongs to
- The Country (C) will be used to indicate what country (Flag State and/or Coastal State) the organisation belongs to

Field	Vessel	Service	User	Organisation
CN (Common Name)	<insert vessel name>	<insert service name>	<insert full name>	<insert organisation name>
O (Organization)	<insert organization ID + name, separated by ";">			
OU (Organizational Unit)	"vessel"	"service"	"user"	"organisation"
C (Country)	<insert organisation country>			

**Table 5 Digital certificates: options for the subject X.500 name fields**

An example for the fields for a vessel certificate could look like:

CN=Mariella, OU=vessel, O=SIN;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 has been used to sign the Subject's certificate. We propose the field consist of the following information, depending on whether the issuer is a (human) user or an organisation<sup>16</sup> (Table 6):

<sup>15</sup> The main difference is that the Maritime Cloud Identity Platform also defines "device" as an additional Subject DN. By devices, they mean "any number of entities that is not covered by the other entity types. It could for example be a lighthouse, an ECDIS or a server that needs to be able to authenticate itself" [31]. We have not defined devices as a potential entity, since we did include device identification and authentication in the design goals in Section 2.3. However, nothing would prevent our proposed PKI architecture from being extended to also include devices if we find it necessary in a later stage of the project

<sup>16</sup> Vessels and services will not operate as Certificate Authorities (CA), however, depending on which PKI architecture is selected (see Section 4) both users (humans) and organisations (i.e. humans acting in behalf of an organisation) could potentially operate their own CA.

Field	User	Organisation
CN (Common Name)	<insert full name>	<insert organisation name>
O (Organization)	<insert organization ID + name, separated by ";">	
OU (Organizational Unit)	"user"	"organisation"
C (Country)	<insert organisation country>	

**Table 6 Digital certificates: options for the issuer (CA) X.500 name fields**

An example for the Issuer (CA) X.500 name fields for a shipowner could look like:

CN=Bedriftsidrettslaget SINTEF, OU=organisation, O=SIN;SINTEF, C==NO

The **Subject Unique ID** and **Issuer Unique ID** fields allows another (optional) way of uniquely identifying the certificate owner. To our knowledge there is no such universally accepted unique identifier that can be used for vessels, services, users and organisations and we therefore propose not to use these fields.

The **Extension** field can be used to store additional information. The Maritime Cloud Identity Platform has proposed to use the "otherName" to tie a vessel certificate to a unique identifier representing the Flag State, Call Sign, IMO number, MMSI number, AIS shiptype, Port of register, MRN and Permission associated with that particular vessel. For user and service certificates, only MRN and Permission will be used in the Maritime Cloud solution. Whether the extension field is necessary for the purposes of the CySiMS project needs to be further discussed in the consortium before a recommendation can be made.

The **Validity Period** field indicates between which dates the certificates are valid. Similar to the extension field, the exact date range that will be recommended by the CySiMS project needs to be further discussed in the consortium before a decision can be made.

Finally, the **Signature Algorithm ID**, **Subject Public Key Info** and **Algorithm ID** fields will depend on the algorithms selected for the PKI. This will be further discussed in the next subsection.

### 3.3 Key material and algorithms

In this section, we present two potential public key algorithms for the CySiMS PKI solution, and discuss some of their strengths and weaknesses. We consider this to be study considerations rather than explicit requirements, since key material and algorithms should be based on predicted usage and operations (focus of D2.2).

The two most prominent public key algorithms are Rivest-Shamir-Adleman (RSA) [22] and Elliptic Curve Cryptography (ECC) [23]. 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 [24], 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 [25]:

*"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 [26] before quantum resistant cryptography is proven and standardised, the quantum resistance approach of CySiMS is to design the PKI in a way that enables migrating to future quantum resistant cryptography without excessive costs or effort.

### 3.4 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 the PKI ecosystem. For shore-based entities (users, organisations and services), a Hardware Secured Module (HSM) installed in the relevant servers is a simple solution, which will offer sufficient security. However, other options exist as well. In this section, we briefly discuss smartcard, HSM and software based solutions in general (section 3.4.1-3.4.3) before we take a further look into potential options for the vessels (section 3.5).

#### 3.4.1 Smartcards

A smartcard is a pocket-size card with embedded integrated circuits. A smartcard provides a tamper-resistant security system, which can be used for storage of the private key(s), is able to permanently store additional data such as certificates, and has built-in processing capabilities that can perform cryptographic functions. The smartcard could 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. By combining a PKI-enabled smartcard with another form of authentication (e.g. a PIN code), the smartcard can be carried around by users or moved from vessel to vessel, without compromising the security of the PKI infrastructure.



### 3.4.2 HSMs

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.

### 3.4.3 Software-based

A fully software based PKI approach is very flexible with regard to the amount of available hardware, and with some additional measures it can be reasonable secure. It 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. The computation of cryptographic functions could be slower than for smartcards and other HSMs depending on the availability of specialised cryptographic functions in the processor.

## 3.5 Practical options for installing the PKI system on vessels

When it comes to installing the PKI system on vessels, there are several options including; using the VDES unit, develop a dedicated PKI unit, or using a general bridge computer.

### 3.5.1 Use the VDES

Since it seems likely that future ships will have a VDES unit, one option for installing the PKI system onboard is to embed the solution on the VDES unit. The functionality would need to be made available to other units on the bridge so that the PKI authentication credentials for the vessel could be shared among the systems on board.

With regard to storing and processing keys on the VDES unit, there are two main options that both require modification to the current VDES design: Smartcard or an integrated HSM chip.

### 3.5.2 Develop a dedicated PKI unit

Designing 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. The downside would be the additional cost of purchase, installation and maintenance compared to utilising other already existing hardware.

With regard to storing and processing keys on a dedicated PKI unit, there are two main options: Smartcard or an integrated HSM chip.

### 3.5.3 Use a conventional bridge computer

Relying on existing hardware where it is possible to install an additional software package is a flexible and cost effective approach allowing all systems and applications to use the same PKI. The downside is additional maintenance burden on the crew or the shipping company, which may require additional technical competence.

With regard to storing and processing keys on a general computer, there are several options: use software and a normal hard drive, use a smartcard through USB, and use a HSM chip.

### 3.6 Certificate Enrolment

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 certificate for the entity's public key and returns the certificate to the entity. This section mainly presents enrolment options for the vessels because enrolment on shore is much more straightforward. The discussion is sectioned by three different options for where to store the certificates and private keys; on a smartcard in the VDES terminal, in software, or in the VDES hardware.

The different alternatives has different strengths and weaknesses, some specific and others more general. For example, in the case of needing to introduce a new root certificate in the PKI system, all the smartcards needs to be replaced, while for software an update might accomplish the same. Then again, it is easier to introduce a malicious root certificate in the software-based alternative.

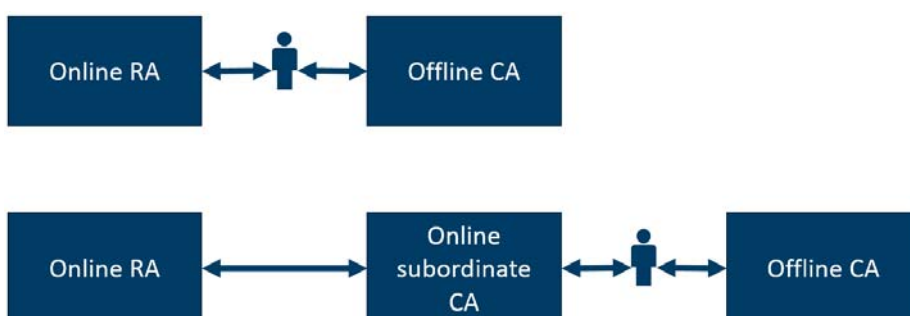
Enrolment of vessels into the PKI will require multiple steps and actors, thus the illustrations in this section uses the colour scheme in Figure 9 to annotate the actions with data exchange, distribution of physical equipment and optional steps respectively. The alternatives illustrate the case of a single root CA for simplicity, but the same enrolment systems would apply to a multi root PKI infrastructure with the addition that the correct CA certificate would have to be provided for storage on the vessel.



**Figure 9 The colours used to annotate the different exchanges of data, equipment and optional steps**

For each of the alternatives in this section, the CA can be can be either online or offline. Figure 10 illustrates the high-level difference between the two setups. When having a fully offline CA, humans must be involved by manually transferring a CSR to the air gapped (offline) CA and finally move the signed certificate from the CA to the RA or a certificate server depending on the setup. Air gapping the CA makes it easier to guarantee the security of the private keys used to issue certificates, but it also increases the amount of required personnel.

Having an online subordinate CA that is signed by an offline root CA, would reduce the amount of required personnel, most likely reduce the time to have a certificate signed and most likely provide sufficient security if implemented correctly. The downside of having an online CA is increased hardware costs and the need to manage two CAs for each CA – one online and one offline. The latter would be touched very rarely.



**Figure 10 The top row illustrates an offline CA where a human must transfer the CSR from RA to CA. The bottom row illustrates a online subordinate CA with an offline CA**

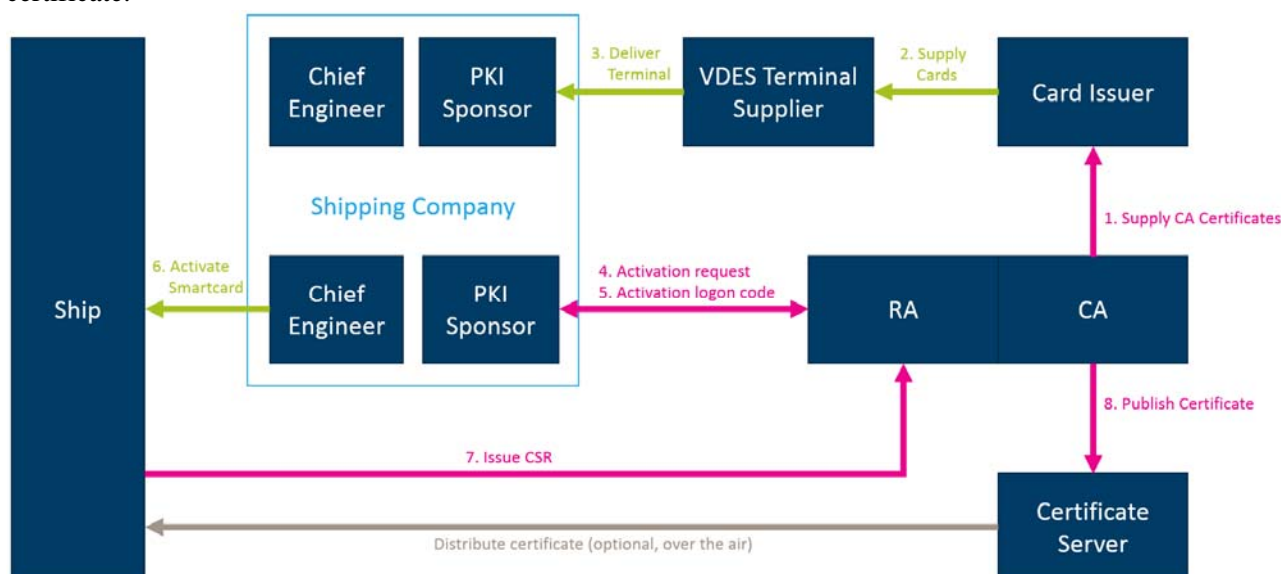


### 3.6.1 Certificate enrolment using smartcard in VDES Terminal

This category of enrolments assumes that the key and certificate store as well as cryptographic functions are placed inside the VDES terminal while still being accessible to other communication utilities and applications on the bridge. Furthermore, smartcards are used to store the root CA certificate and a pre-generated set of key pairs.

#### 3.6.1.1 Alternative 1

In this alternative, the root certificate of the online CA is provided to the smartcard issuer to be embedded in any smartcards they produce. The smartcards are transmitted to the VDES terminal supplier for inclusion so that the ship owner or engineer never has to handle the smartcards. Upon an order from the shipping company, the terminal is delivered for installation. Upon receiving the terminal, the PKI sponsor of the shipping company provides the Registration Authority (RA) with the necessary details and requests that the smartcard is activated. Upon receiving such a request, the RA provides the PKI sponsor with a logon code, which the engineer of the ship uses to activate the card. After the card has been activated, the VDES terminal creates a Certificate Signing Request (CSR) by fetching relevant information from the ship, such as its IMO number, and sends the CSR to the RA. The RA validates the CSR against information received from the PKI sponsor and passes it along to the Certificate Authority (CA) for the actual signing of the certificate. The CA publishes the certificate on a certificate server from which the VDES terminal on the ship can fetch its new certificate.



#### Pros

- Smartcards offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge

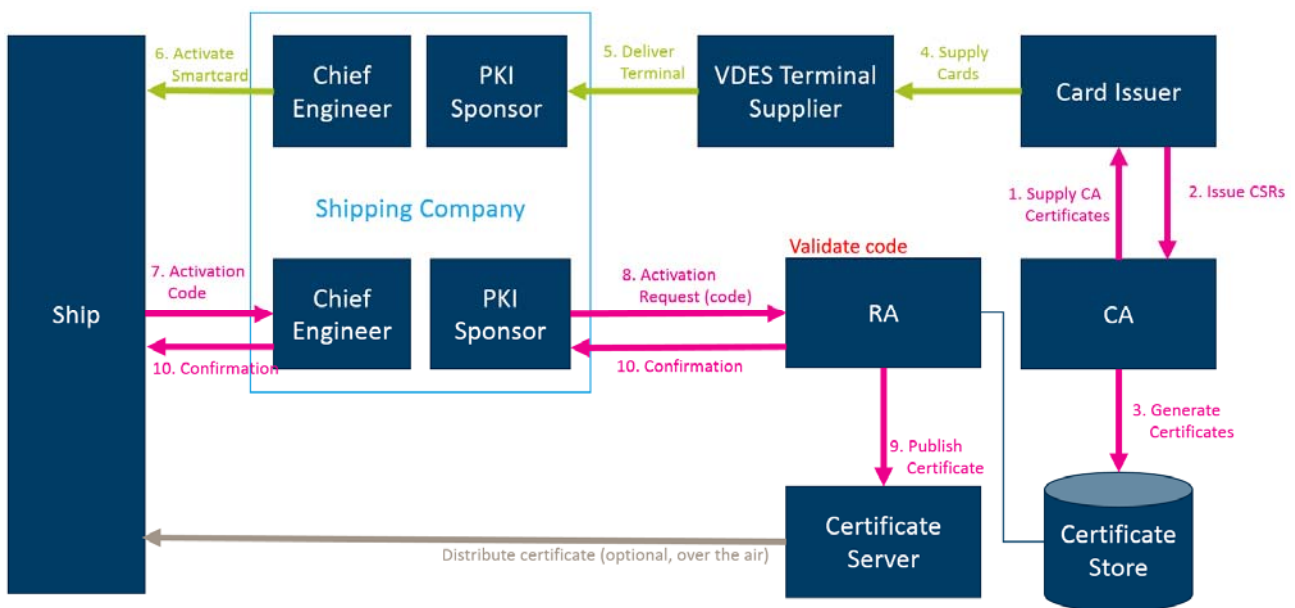
#### Cons

- The solution does not use pre-generated key pairs, which increases the risk of unauthorised certificate signatures
- The engineer might not have the required competence to set up the PKI solution

#### 3.6.1.2 Alternative 2

This alternative assumes that the smartcards are produced after the PKI sponsor of a shipping company has ordered a new VDES terminal. The offline CA provides the smartcard issuer with the root CA certificate to

be included on every smartcard. Since the smartcard producer knows in which vessel the smartcard is to be used, a CSR is issued for the relevant vessel. The CA immediately signs the certificate and adds it to a certificate store, which is not accessible outside the PKI Operator. The smartcard issuer provides the correct smartcard to the VDES terminal supplier, which must ensure that the terminal in which the smartcard is installed will be installed in the correct vessel. When the VDES terminal is installed, the smartcard is activated, and the VDES terminal generates an activation code (based on vessel data, mostly public information such as the IMO number), which the PKI sponsor must provide to the RA. If the code is valid, the pre-generated certificate will be moved from the certificate store to the certificate server from where the ship can fetch it.



## Pros

- Smartcards offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- Additional verification of installation on correct vessel makes it more difficult for an attacker to trick the PKI sponsor into activating a stolen VDES terminal

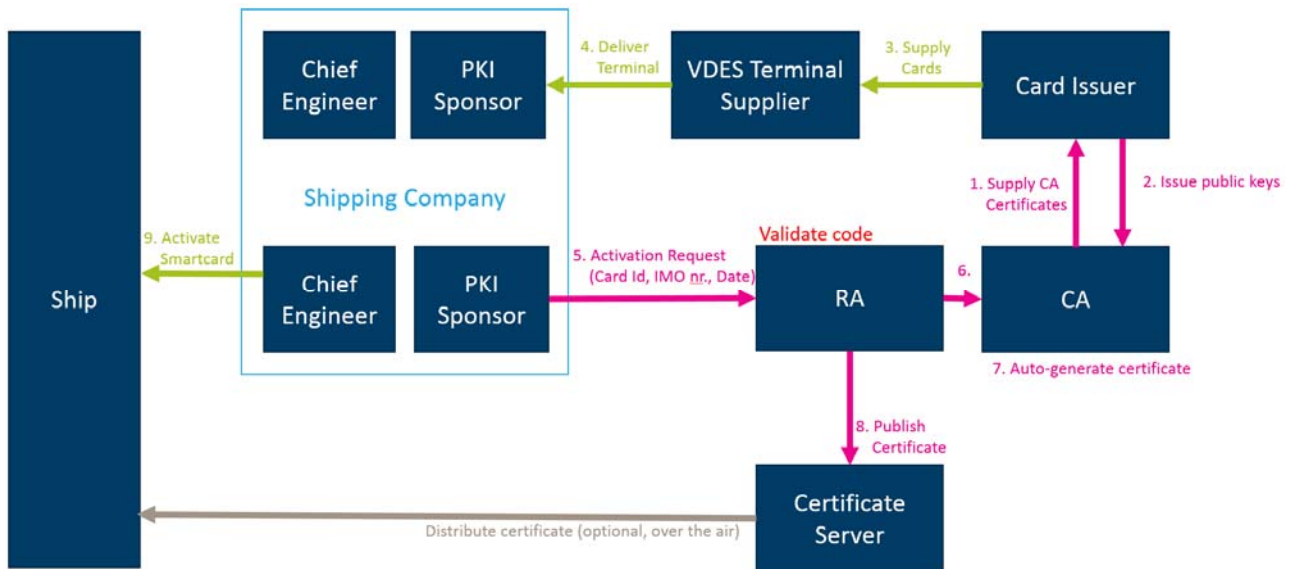
## Cons

- Longer time of delivery since the vessel and company details must be known before the smartcard leaves its producer
- Requires advanced logistics to know that the correct smartcard and VDES terminal enters the correct vessel
- Likely to be easy for an attacker to emulate correct data and thus obtain a valid activation code

### 3.6.1.3 Alternative 3

This alternative has similarities with alternative 2, but differs in some important aspects. It starts off by having the root CA provide the smartcard manufacturer with the root certificate for inclusion on the produced smartcard. The smartcard issuer now generates a set of key pairs on the smartcard, extracts the public keys and sends these, together with the corresponding serial number of the smartcard, to the PKI Operator. The smartcard is then passed along to the VDES terminal supplier, which can place any smartcard in any terminal on any vessel. The PKI sponsor then sends an activation request to the RA containing the

relevant information for the certificate. The RA validates the received activation request, and the CA generates a corresponding certificate based on the first active public key belonging to the smartcard with the provided serial number. This certificate is published on the certificate server for the ship to fetch. Finally, an engineer can activate the smartcard.



## Pros

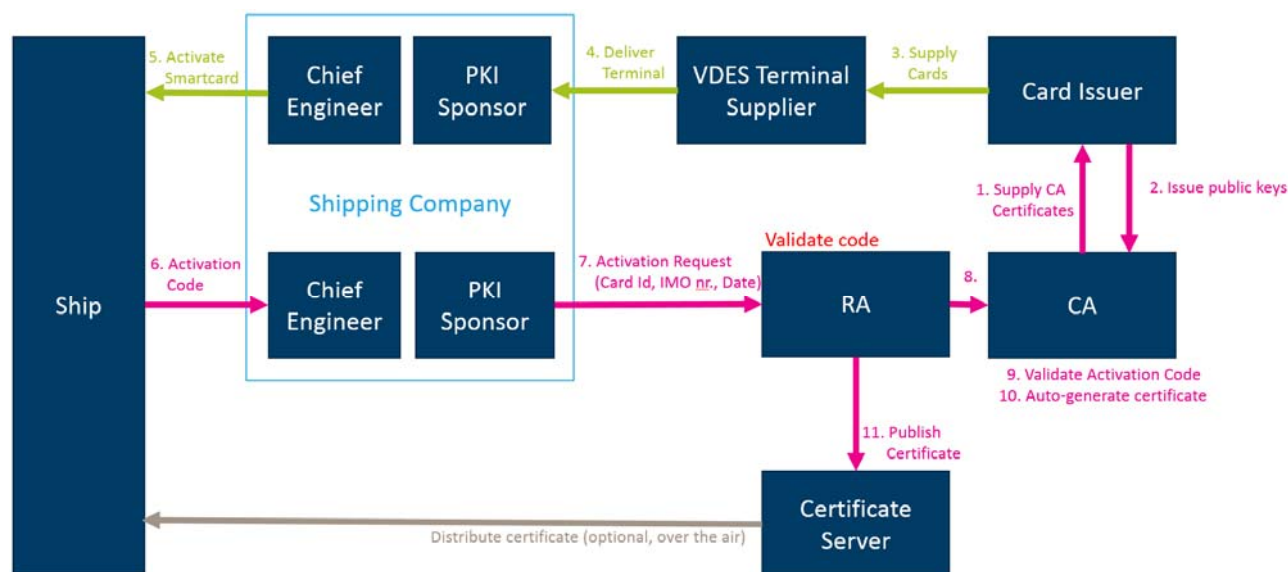
- Smartcards offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which smartcard)
- Since the smartcards are not tied to specific vessels they can be installed on any vessel
- More efficient supply line than alternative 2

## Cons

- The certificate sponsor must provide information such as smartcard serial number and IMO number to the RA in addition to this information being available to the VDES terminal. This introduces an additional source of errors
- The engineer might not have the required competence to set up the PKI solution

### 3.6.1.4 Alternative 4

This alternative is similar to alternative 3, but the smartcard is activated as soon as the terminal is installed and an activation code (likely to contain card id, IMO number, date, etc.) is provided to the PKI sponsor for inclusion with the activation request.



## Pros

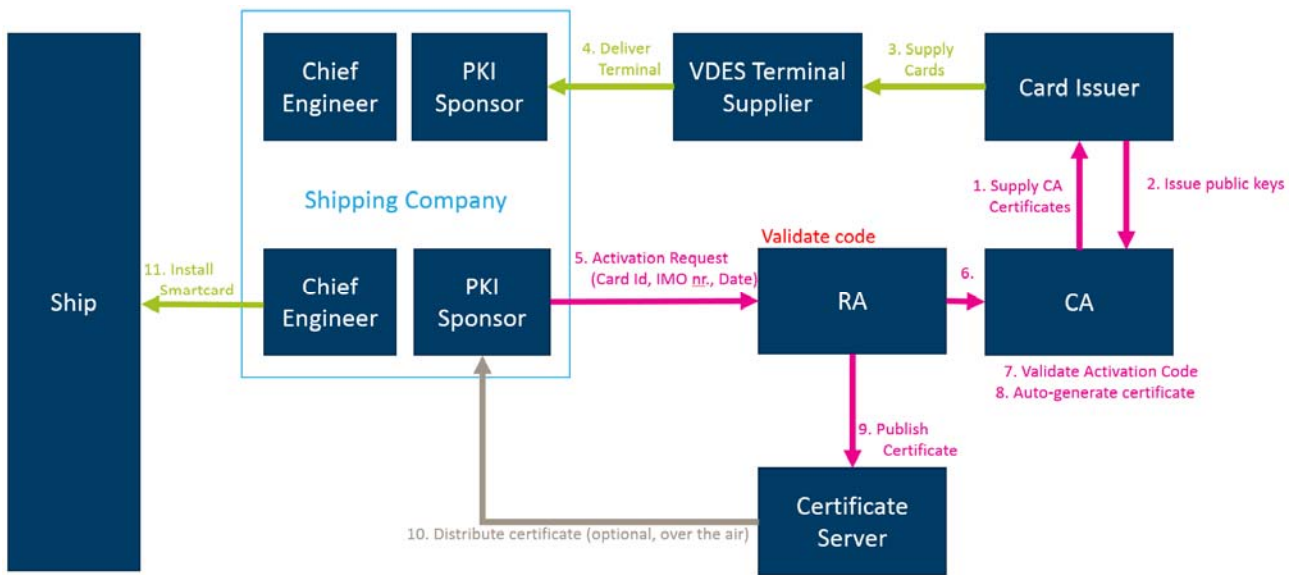
- Smartcards offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- Additional verification of installation on correct vessel makes it more difficult for an attacker to trick the PKI sponsor into activating a stolen VDES terminal
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which smartcard)

## Cons

- The certificate sponsor must provide information such as smartcard serial number and IMO number to the RA in addition to this information being available to the VDES terminal. This introduces an additional source of errors
- The engineer might not have the required competence to set up the PKI solution
- Likely to be easy for an attacker to emulate correct data and thus obtain a valid activation code

### 3.6.1.5 Alternative 5

This alternative moves the activation and certification process from the vessel to the PKI sponsor. The CA provides its root certificate to the smartcard issuer and the smartcard issuer provides the CA with public keys mapped against the serial number of the smartcard. The smartcard is sent to the VDES terminal supplier, which installs the smartcard in the terminal and delivers it to a shipping company upon order. The PKI sponsor crafts a activation request containing information such as the smartcard ID, the IMO number of the vessel in question and the date of the request. The RA validates the request and the CA signs a certificate based on the pre-generated public keys and publishes the certificate on the certificate server. Now, the PKI sponsor can obtain the certificate, install it on the VDES terminal and finally have the engineer install the terminal on the vessel.



## Pros

- Smartcards offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- The PKI sponsor can inspect and validate the certificate before it is installed on the VDES terminal
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which smartcard)

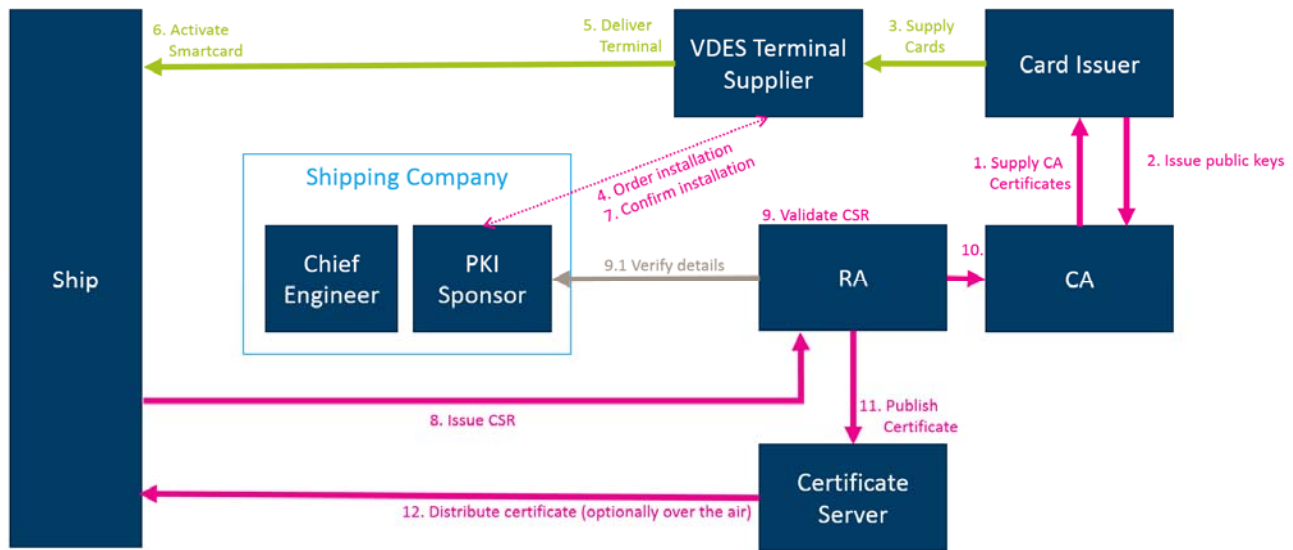
## Cons

- Requires technical competence regarding PKI management in all the shipping companies
- The engineer might not have the required competence to set up the PKI solution

### 3.6.1.6 Alternative 6

In this alternative, most of the responsibilities are moved to the VDES terminal supplier, the RA and the VDES terminal itself.

As in the prior alternative, the CA provides its root certificate to the smartcard issuer, which embeds the root certificate on all smartcards, generates a set of key pairs and sends the public keys mapped against the smartcard's serial number to the PKI Operator. The smartcards are then sent to the VDES terminal supplier, which installs the smartcards in the terminal. When a PKI sponsor orders a new terminal for one of the company's vessels, the terminal supplier already has them in store and can install the terminal on behalf of the customer. After installation, the terminal supplier activates the smartcard and confirms to the customer that the installation is complete. The VDES terminal gathers the necessary data and crafts a CSR, which it sends to the RA. The RA validates the CSR and can optionally verify that the details are correct by contacting the PKI sponsor responsible for the vessel in question. Upon accepting the CSR, the CA signs the certificate and publishes it on the certificate server. Finally, the VDES terminal fetches the newly signed certificate from the certificate server.



## Pros

- Smartcards offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- The solution does not require any technical competency regarding PKI management in the shipping companies or amongst the crew on the vessels
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which smartcard)

## Cons

- The shipping company is more dependent on the VDES terminal supplier, since the supplier is also responsible for installing and activating the terminal

### 3.6.2 Certificate enrolment using software

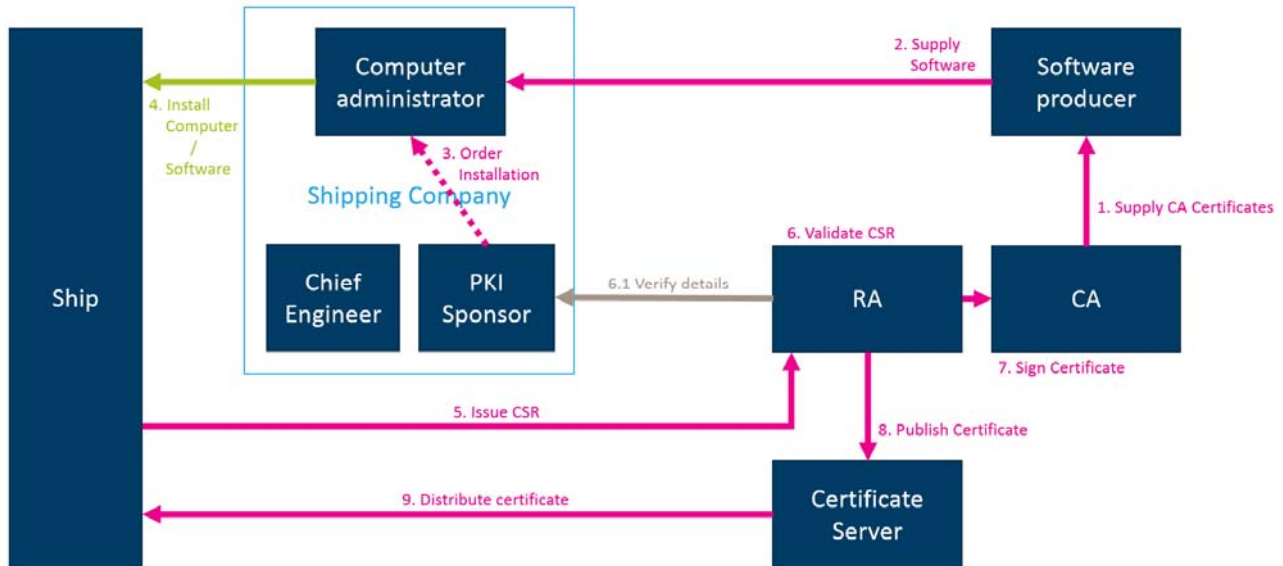
This category of enrolment alternatives assume that the key and certificate store as well as cryptographic functions is fully software based and provides its capabilities to other systems on the bridge through running on a local computer on board the vessel. This alternative provides less security than the alternatives in Section 3.6.1 and 3.6.3 due to not having a secure storage for the private keys and the root CA certificate(s), but on the other hand, it requires fewer involved actors. A software producer creates the software and bundles it with the root CA certificate into an installation package that can be executed on computers for installation.

#### 3.6.2.1 Alternative 7

In this alternative, the CA provides the root CA certificate to the software producer that incorporates the certificate in the installation package. The software producer supplies the installation package to the computer administrator of the shipping company, which installs the software on a vessel upon the order of the PKI sponsor. During installation, the software collects the necessary information about the vessel, creates



a CSR and sends it to the RA. The RA validates the CSR, potentially by contacting the relevant PKI sponsor for additional verification, and passes it on to the offline CA for signing of the certificate. When the certificate has been signed, the RA publishes it on the certificate server from where the software can obtain a copy.



## Pros

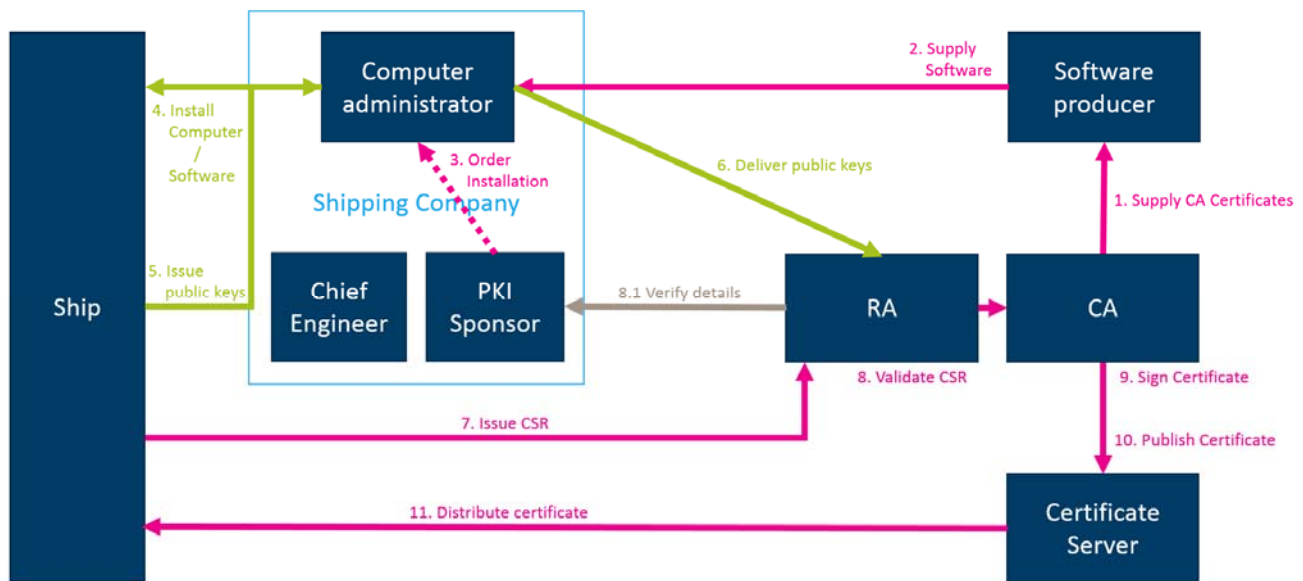
- This solution involves fewer actors and may hence be more cost-efficient and more flexible
- Most vessels already have computers available that could be used to host the PKI software
- Easy to distribute new root CA certificate if the existing root CA certificate expires or is compromised

## Cons

- Less secure storage of keys and root CA certificate than the alternatives in Section 3.6.1 and 3.6.3
- The solution does not use pre-generated key pairs, which increases the risk of unauthorised certificate signatures
- Requires high technical competence on maintaining secure computer systems in each shipping company

### 3.6.2.2 Alternative 8

This alternative is similar to alternative 7, but after installing the computer or software on the vessel, the computer administrator receives a set of public keys from the software that he needs to transfer to the RA by a different channel of communication. The purpose of this is to allow the RA to verify that the public key in a CSR is among those delivered by the shipping company.



### Pros

- This solution involves fewer actors and may hence be more cost-efficient and more flexible
- Most vessels already have computers available that could be used to host the PKI software
- Easy to distribute new root CA certificate if the existing root CA certificate expires or is compromised
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which ship)

### Cons

- Less secure storage of keys and root CA certificate than the alternatives in Section 3.6.1 and 3.6.3
- Requires high technical competence on maintaining secure computer systems in each shipping company
- Using an alternate channel of communication to transfer public keys to the RA may introduce an additional source of errors

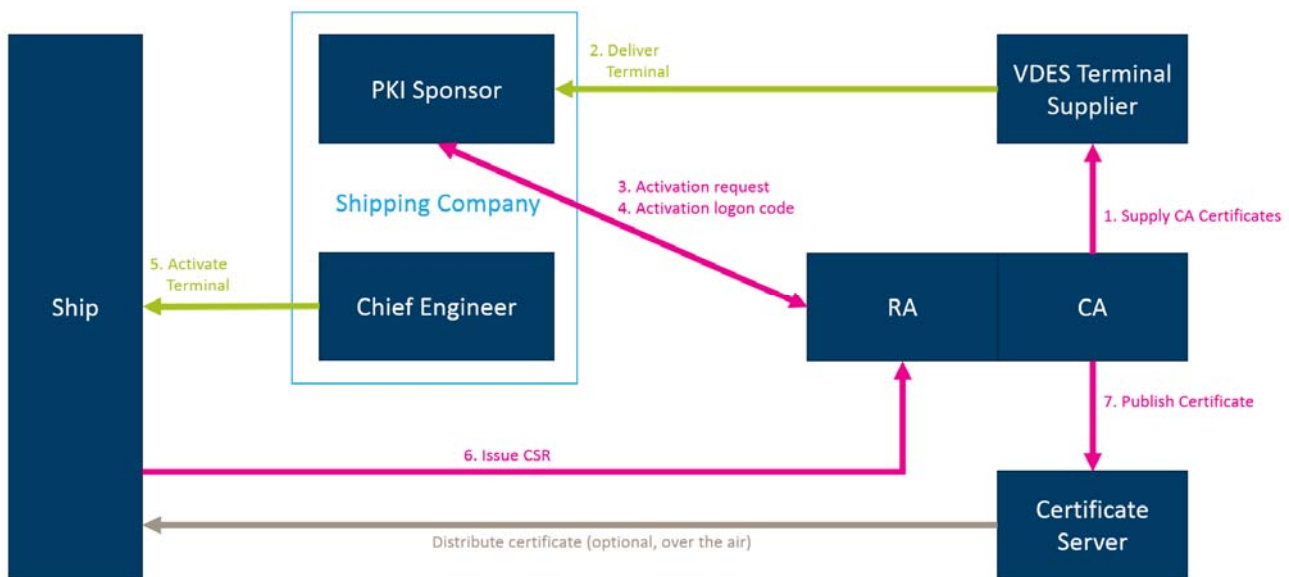
### 3.6.3 Certificate enrolment using VDES Hardware

This category of enrolment alternatives are quite similar to the first category (smartcard in VDES terminal, described in Section 3.6.1) in that it uses the VDES terminal, but here we utilise the current hardware and a Hardware Security Module (HSM) on the terminal. This could be an embedded chip on the unit or a USB HSM unit. The security of the alternatives presented in this subsection relies fully on the trustworthiness of the VDES terminal supplier and its hardware.

#### 3.6.3.1 Alternative 9

The CA provides the root CA certificate to each VDES terminal supplier for inclusion. The terminal supplier delivers the VDES terminal to the shipping company where the PKI sponsor sends an activation request to the RA. The RA provides an activation code and the engineer installs and activates the terminal on the ship. At this time, the terminal generates a CSR and sends it to the RA. The RA validates the CSR and requests the CA to sign the certificate and publish it on the certificate server.





### Pros

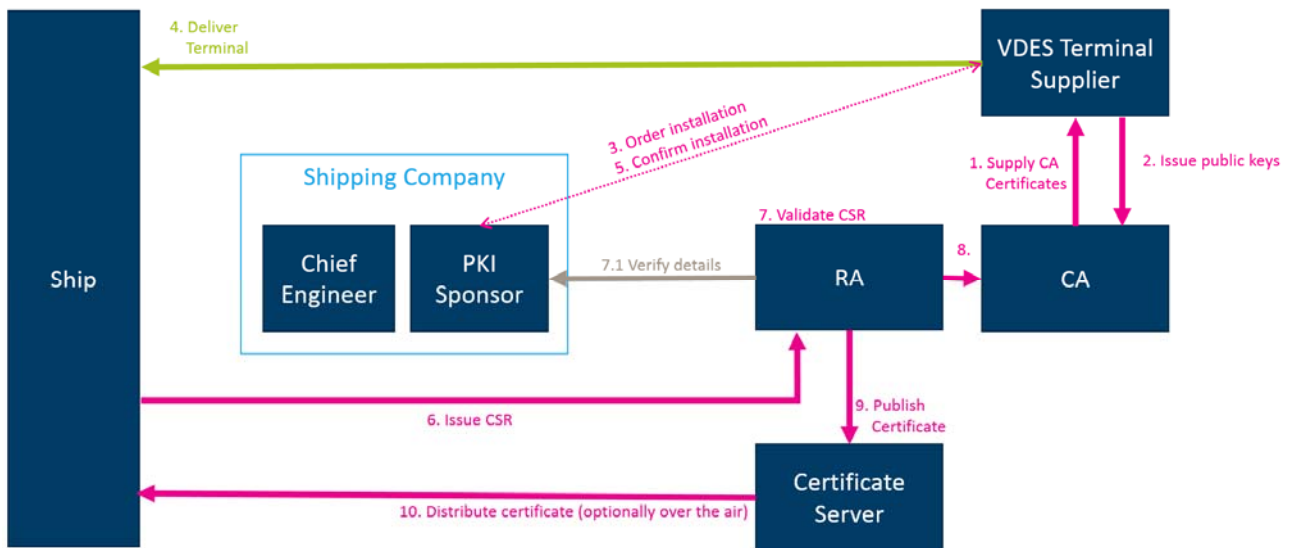
- HSMs offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- Fewer actors involved than in the alternatives in Section 3.6.1

### Cons

- The solution does not use pre-generated key pairs, which increases the risk of unauthorised certificate signatures
- The engineer might not have the required competence to set up the PKI solution
- Other equipment on the vessel will be dependent on the VDES terminal in order to set up a secure communication link and to sign or verify digital signatures

#### 3.6.3.2 Alternative 10

This alternative is similar to alternative 6, but it is using an integrated HSM chip rather than a smartcard. The CA provides the root CA certificate to the VDES terminal supplier for inclusion on every unit and generates a set of key pair on the HSM. The public keys are then exported and provided to the PKI Operator with an identification of the specific terminal. The terminal supplier now has VDES terminals in store that are ready for installation on any vessel. After the certificate sponsor of a shipping company orders the installation of a terminal, the terminal supplier installs the terminal on the correct vessel and sends a confirmation of this to the certificate sponsor. The installed terminal collects the necessary information, generates a CSR and sends it to the RA. The RA validates the CSR, potentially also verifying the information with the PKI sponsor of the vessel in question, and passes the CSR to the CA for signing of the certificate. The signed certificate is made available on the certificate server for the vessel to collect.



## Pros

- HSMs offer a tamper-proof solution for the vessels
- No additional hardware installations necessary on the bridge
- Requires no technical competency regarding PKI management in the shipping companies or amongst the crew on the vessels
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which smartcard)
- Fewer actors involved than in the alternatives in Section 3.6.1

## Cons

- The shipping company is more dependent on the VDES terminal supplier since the supplier is also responsible for installing and activating the terminal
- Other equipment on the vessel will be dependent on the VDES terminal in order to set up a secure communication link and to sign or verify digital signatures

### 3.6.4 Certificate enrolment using dedicated PKI unit

This category of enrolment alternatives are quite similar to the last category (Certificate enrolment using VDES Hardware, described in Section 3.6.3) in the enrolment options if it is decided to use an integrated HSM. Alternatively, an external smartcard reader could be combined with software on the unit.

#### 3.6.4.1 Alternative 11

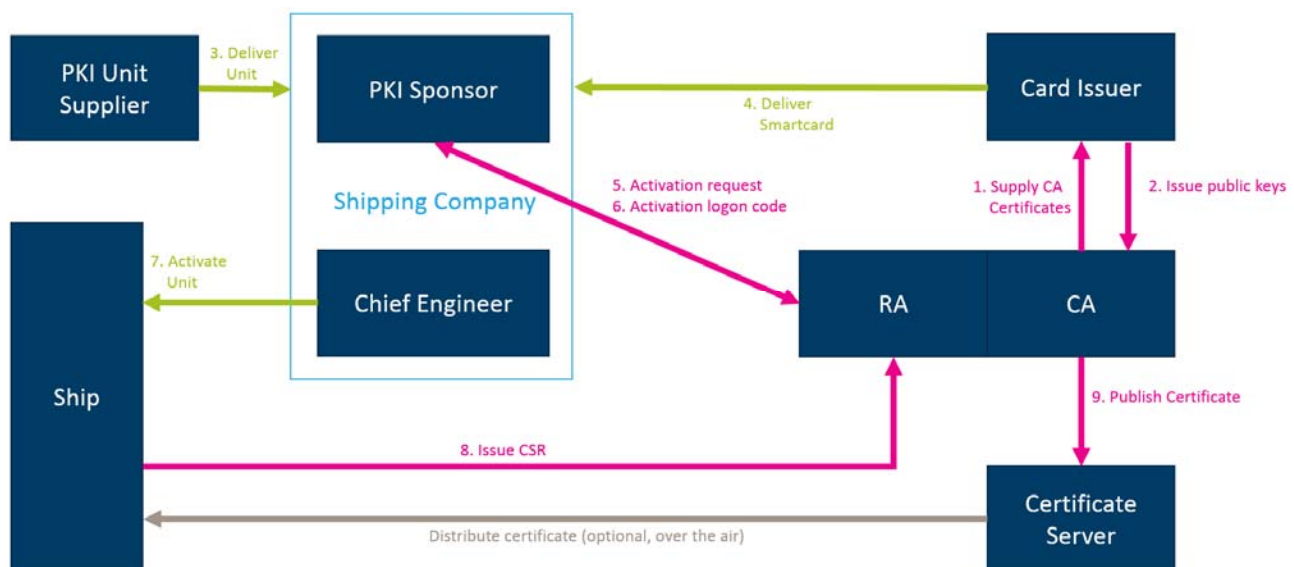
Equal to alternative 9, but the VDES terminal supplier is substituted by a PKI unit supplier.

#### 3.6.4.2 Alternative 12

Equal to alternative 10, but the VDES terminal supplier is substituted by a PKI unit supplier.

### 3.6.4.3 Alternative 13

This alternative separates the keys from the actual PKI unit. First, the PKI Operator provides the root certificate to the card issuer, which generates key pairs, exports the public keys and sends them to the PKI Operator. Next, the PKI Sponsor receives a PKI unit from the PKI Unit Supplier and a smartcard from the Card Issuer. The PKI Sponsor sends an activation request with the relevant vessel details to the RA and receives back an activation code. Now, the engineer can install the unit and activate it using the received activation code. Finally, the unit generates a CSR, sends it to the RA which validates it and has the certificate signed.



#### Pros

- Smartcards offer a tamper-proof solution for the vessels
- The solution uses pre-generated key pairs, which makes it more difficult for an attacker to get unauthorised certificates signed (the RA knows which public keys belong to which smartcard)
- The PKI Unit is independent from other systems on the vessel which might make it more acceptable and modular
- A simple and independent solution

#### Cons

- Requires technical competence regarding PKI management in all the shipping companies

### 3.6.5 Enrolment summary

Table 7 provides an overview over the different certificate enrolment alternatives. The table includes information on where and how the private keys are generated, and how they will be transported and stored at the entities.

Alt	CA Certificate		End Entity Private key			End Entity Public key			CSR/Activation	End Entity Certificate	
	Transport	Storage	Generation	Transport	Storage	Pre gen.	Transport	Storage		Transport	Storage
VDES + SC											
1	SC	SC	SC, VDES	n/a	SC	✖	n/a	SC	Activation PKI sponsor + CSR VDES	Online	SW/HSM/SC
2	SC	SC	CA	SC	SC	✓	SC	SC	Activation PKI sponsor	Online	SW/HSM/SC
3	SC	SC	SC / Card Issuer	SC	SC	✓	SC	SC	Activation PKI sponsor	Online	SW/HSM/SC
4	SC	SC	SC / Card Issuer	SC	SC	✓	SC	SC	Activation PKI sponsor	Online	SW/HSM/SC
5	SC	SC	SC / Card Issuer	SC	SC	✓	SC	SC	Activation PKI sponsor	Online	SW/HSM/SC
6	SC	SC	SC / Card Issuer	SC	SC	✓	SC	SC	CSR from VDES	Online	SW/HSM/SC
Software											
7	SW	SW	SW	n/a	SW	✖	n/a	SW	CSR SW	Online	SW
8	SW	SW	SW	n/a	SW	✓	SW	SW	CSR SW	Online	SW
VDES + HW HSM											
9	HSM	HSM	HSM	HSM	HSM	✖	HSM	HSM	CSR VDES	Online	HSM
10	HSM	HSM	HSM	HSM	HSM	✓	HSM	HSM	CSR	Online	HSM
Dedicated PKI Unit + SC											
11	HSM	HSM	HSM	HSM	HSM	✖	HSM	HSM	CSR PKI Unit	Online	HSM
12	HSM	HSM	HSM	HSM	HSM	✓	HSM	HSM	CSR	Online	HSM
13	SC	SC	SC / Card Issuer	SC	SC	✓	SC	SC	CSR	Online	SC

**Table 7 An overview over the different certificate enrolment alternatives**

### 3.7 Rekeying

One of the trade-offs in designing a PKI solution is which length of keys to use for which length of time. The larger the keys, the longer they can be assumed to be secure, but longer keys cause a larger overhead on the network and require more powerful processing systems. Therefore, keys of different sizes will have different periods of validity. For the root CA certificate, the period between each rekeying might be as long as 20 years, while for the vessels the validity period might be as low as a few years. This means that the vessel certificates will need to be replaced regularly. For the certificate enrolment alternatives in section 3.6 that rely on pre-generated key pairs stored on a secure element (smartcard or HSM), this process is rather simple, automatic and secure since the PKI Operator already knows all public keys that belong to a vessel and the PKI Sponsor has already guaranteed that the current information is correct. For the alternatives that do not use pre-generated key pairs, rekeying will be a more complicated process where new keys must be generated, the PKI Operator must verify the key and vessel details with the PKI Sponsor and finally a new certificate is downloaded to the PKI System on the vessel.

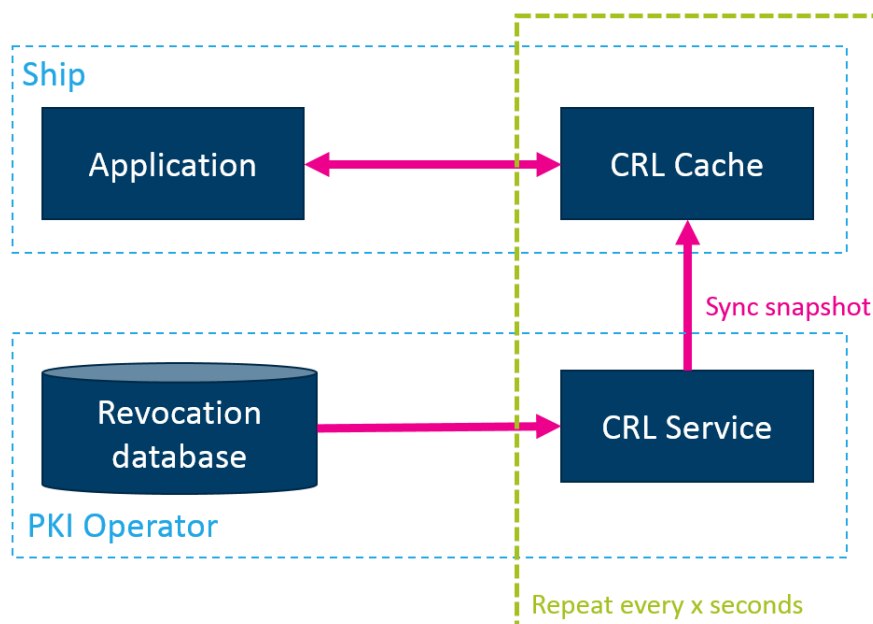
### 3.8 Certificate Revocation

As mentioned in Section 1.2, certificates are generally valid until the certificate expires. Due to the possibility of losing control of the private key or an actor misusing an issued certificate, mechanisms for invalidating a certificate that has not yet expired needs to be in place. This is called certificate revocation. This section will introduce the different revocation methods that exist, and discuss their respective strength and weaknesses.

#### 3.8.1 Certificate Revocation List

The most common approach to manage certificate revocation in a PKI infrastructure is to use Certificate Revocation Lists (CRLs) [20]. The CRLs are distributed periodically to the relevant entities and contains the entire list of revoked certificates. For each revoked certificate, the CRL includes a serial number and the reason why the certificate was revoked. The available reasons for revocation includes: "unspecified", "key compromise", "CA compromise", "affiliation changed", "superseded", "cessation of operation", "certificate hold", "remove from CRL", "privilege withdrawn", and "AA compromise". The *remove from CRL* reason may only occur if the received CRL is a delta on an earlier version. A delta CRL lists only those certificates which have changed status since the last complete CRL. A CRL must always be signed by the issuing CA in order to be valid. Expired certificates can be excluded when generating a new CRL.

Figure 11 shows the process of controlling if a certificate is revoked or not using CRLs. The local entity, that being a ship or a shore unit, maintains a local copy of the complete CRL, allowing it to check any certificate against the local cache. Periodically the central CRL of the PKI operator will be transferred to the local unit. Given that the transfer of the central CRL repository to the local cache only happens periodically, the local cache might not be updated with the latest revoked certificates when the entity checks whether a particular certificate is valid or not. Still, the existence of the local cache allows an actor to rely on the content of a CRL while being in areas without an adequate connection to download newer versions. The longer a ship is offline, the less it can trust that the CRL is fully updated and complete. This is a trade-off that will need to be considered with regard to available connectivity, bandwidth and how important it is for the CRL to always be fully updated.



**Figure 11** The process of checking the validity of a certificate from a ship using CRLs

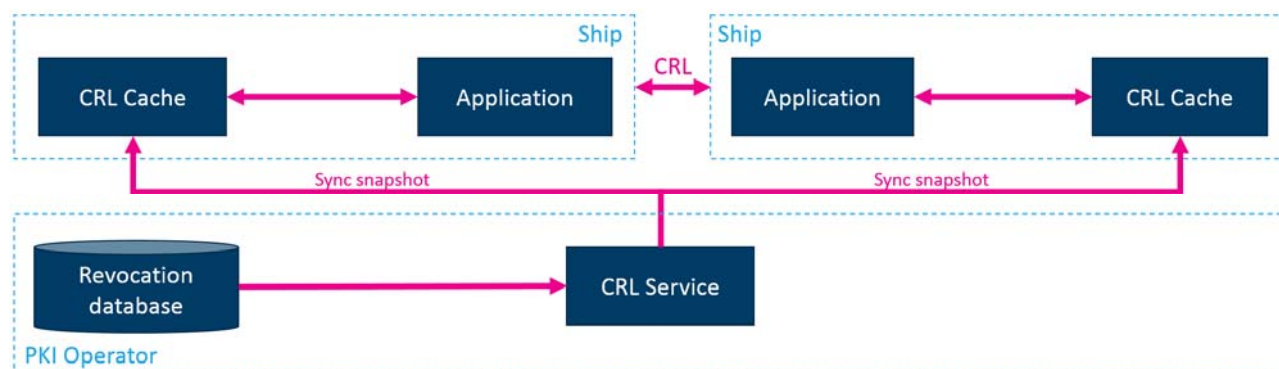
## Pros

- The CRL solutions can be used by entities that are offline during long periods of time
- An entity using a CRL to check whether a certificate is valid or not will get an immediate response

## Cons

- After some time, the CRLs might become large due to aggregated revocations. While the time between each sync can be configured, a potentially large amount of data will have to be downloaded regularly
- Depending on how often the CA issues a new CRL, the latest official CRL might not be updated with the latest revocations

In order to increase the likelihood that all the entities hold the last version of the CRL at all times, it is possible to reuse a mechanism of eventual consistency [27] from distributed computing and thus allow the synchronisation to happen between the PKI Operator's CRL Service (master) and the entities, but also allowing synchronisation to happen between other entities in the ecosystem. For example, when two ships initiate a communication, they could provide the serial numbers of their own version of the CRL to each other. If one of the ships has a newer version of the CRL than the other ship, this CRL could be transferred to the ship holding the older CRL. This is illustrated in Figure 12. This could increase the interaction between actors in near proximity of each other, but also allow for reduction in total download size of CRLs since each actor will be carrying the CRLs for his CA and could provide these to anyone he interacts with. Thus, vessels would not necessarily have to download all CRLs periodically. Otherwise, this option has the same offline properties and trade-offs as traditional CRL distribution.



**Figure 12** Eventually consistent CRLs with synchronisation between ships and periodical sync from the CRL Service

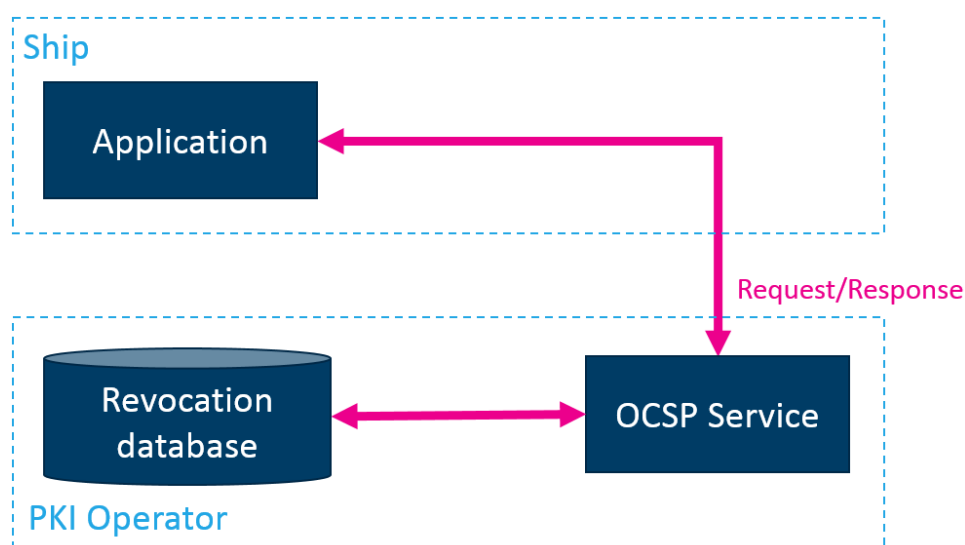
### 3.8.2 Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP) [28] is an alternative to CRLs that requires less network capacity and processing power on the receiving units. By sending a minimal amount of information to the OCSP service, like the OCSP protocol version and the identifier of the certificate to be validated, the sender receives a response of valid, revoked or unknown on the certificate in question.

Figure 13 shows the process of verifying the validity of a certificate using OCSP. Upon receiving a certificate, the entity creates a small request to the OCSP service, which in turn queries the central revocation database of the PKI Operator and returns a signed response of "good", "revoked" or "unknown".

Due to a design weakness in OCSP (the fact that the specification requires error messages from the OCSP services to be unsigned), it is possible to block all the revocation queries from clients. This has lead web browsers, which are the most common users of OCSP, to implement CRLs as a fall-back solution, as can be seen in Figure 14.

OCSP requires constant connectivity in order to be operational, and will not support actors being offline.



**Figure 13** The process of checking the validity of a certificate from a ship using the OCSP

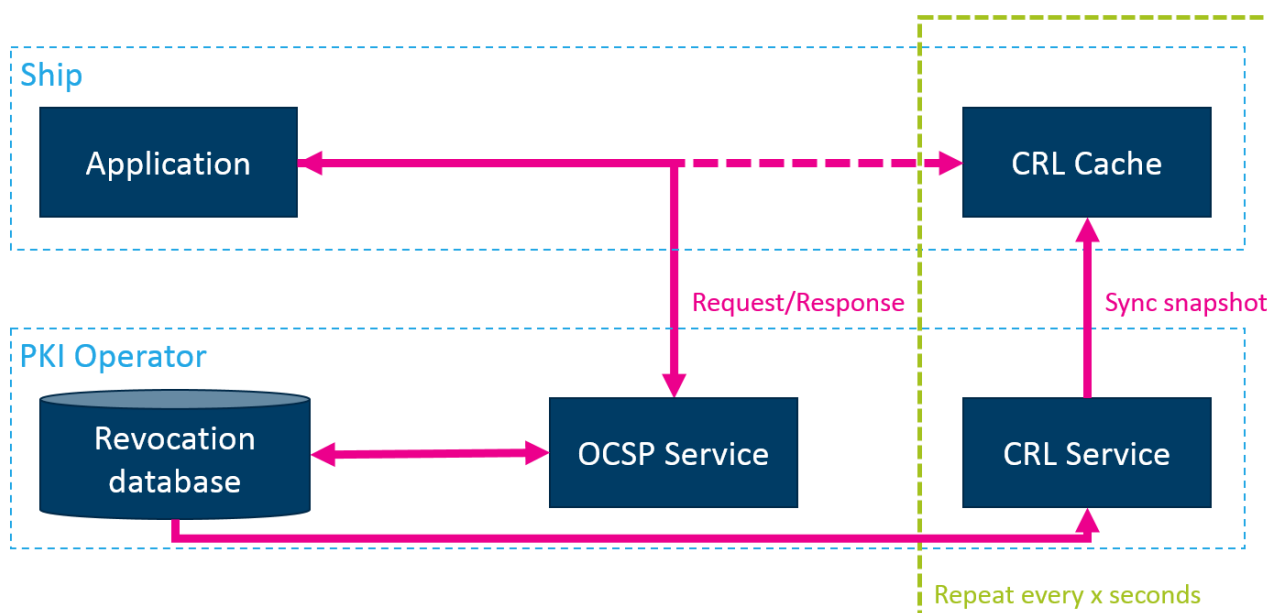


## Pros

- The entities will always have access to updated certificate status
- The small format of the requests and responses means that only little bandwidth will be used

## Cons

- The entities must be online to be able to check the status of a certificate
- It is possible to block all the revocation queries from clients since error messages are not to be signed
- Since the certificate status has to be checked every time an entity receives a certificate, there is a risk of unsolicited surveillance



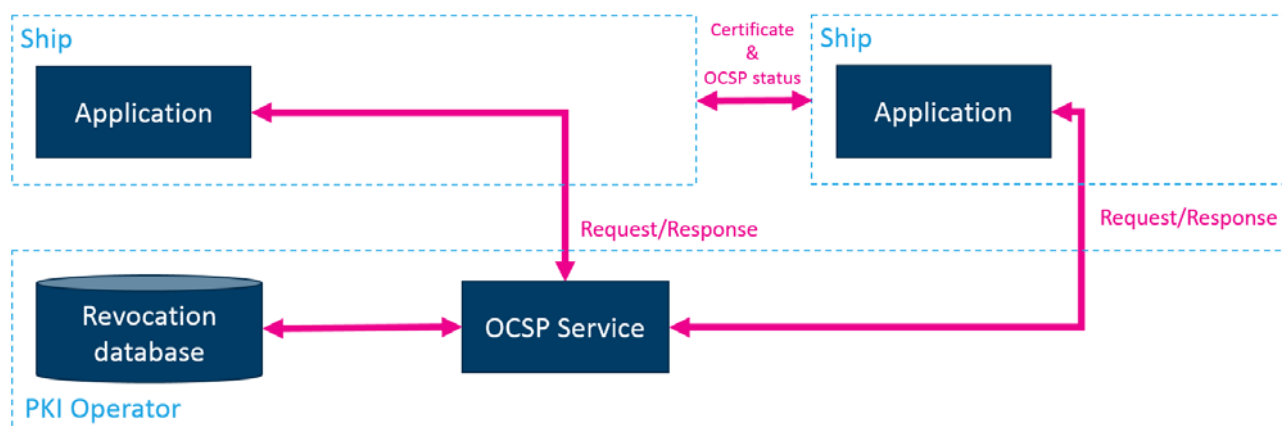
**Figure 14 OSCP certificate validity checking with CRL fallback. The local CRL Cache is only used if no response can be obtained from the OCSP Service**

### 3.8.3 Stapled OSCP

Stapled OSCP [29], [30] is similar to the "ordinary" OSCP described in Section 3.8.2, but in order to reduce the load on the central OCSP service each time a handshake is initiated between two actors both must include a timestamped and CA signed OSCP status response for their own certificate.

Figure 15 shows how each certificate holder would obtain an adequately new status message, signed by the CA, which they provide alongside their own certificate in any certificate handshake involving another actor.

Depending on for how long one allows a stapled OSCP message to be valid, this solution would have different levels of support for a vessel being offline. With a short validity period, the support for offline vessels is near non-existent. As one increases the validity period of a stapled OSCP message, the support for offline vessels also increase.



**Figure 15 Stapled OCSP: Each certificate owner obtains a signed status of their own certificate which they provide alongside their certificate in any certificate handshake**

### Pros

- The entities will always have access to updated certificate status
- The small format of requests and responses means that only little bandwidth will be used
- The number of network requests is limited by the number of issued certificates

### Cons

- The entities must be online sufficiently often to be able to obtain a signed status of their own certificate
- The common use of protocol is for network requests, it *might* therefore not be the best fit for the digital signature use cases

Stapled OCSP can be combined with virally distributed CRLs to provide a backup if an adequately new stapled OCSP could not be obtained. It does, however, add some additional complexity. This would provide the offline benefits of the CRL with the more updated data of the stapled OCSP messages, and could allow for CRLs to be synced more seldom than what would otherwise be required.

### 3.8.4 Certificate Revocation summary

In Table 8, some of the properties of the alternatives discussed above are summarised with the addition of best and worst case values for size. Here we assume, for the sake of the calculations, that a CRL will be valid for one week, a Stapled OCSP will be valid for three days, and a vessel PKI certificate will be valid for three years. Furthermore, we assume the key is ECC with 384 bit for vessel PKI certificates and 384 bit for the CA certificate.

Further assumptions:

- 39 costal states
- 20 000 shipping companies
- 100 000 vessels
- Worst case amount of revoked certificates per CA is 200 certificates

	Size per unit		Unit Count		Download per week per vessel		Total download per week	
	Best case	Worst case	Best case	Worst case	Best case	Worst case	Best case	Worst case
CRL <sup>17</sup>	326 B	3.8 KB	1	20 041	326 B	75 MB	32.6 MB	7.5 TB
Eventually consistent CRL	Similar to CRL, but with more options for reducing the required downloads and load on the central network							
OCSP	514 B	514 B	1	120 041	1 028 B	123 MB	103 MB	12 TB
OCSP + CRL	840 B	4.2 KB	2	140 080	1 354 B	198 MB	135 MB	20 TB
Stapled OCSP	514 B	514 B	1	1	1 028 B	1028 B	103 MB	103 MB
Stapled OCSP + CRL	840 B	4.2 KB	2	20 041	1 354 B	75 MB	135 MB	7.5 TB

**Table 8 Estimates of network requirements for different revocation solutions**

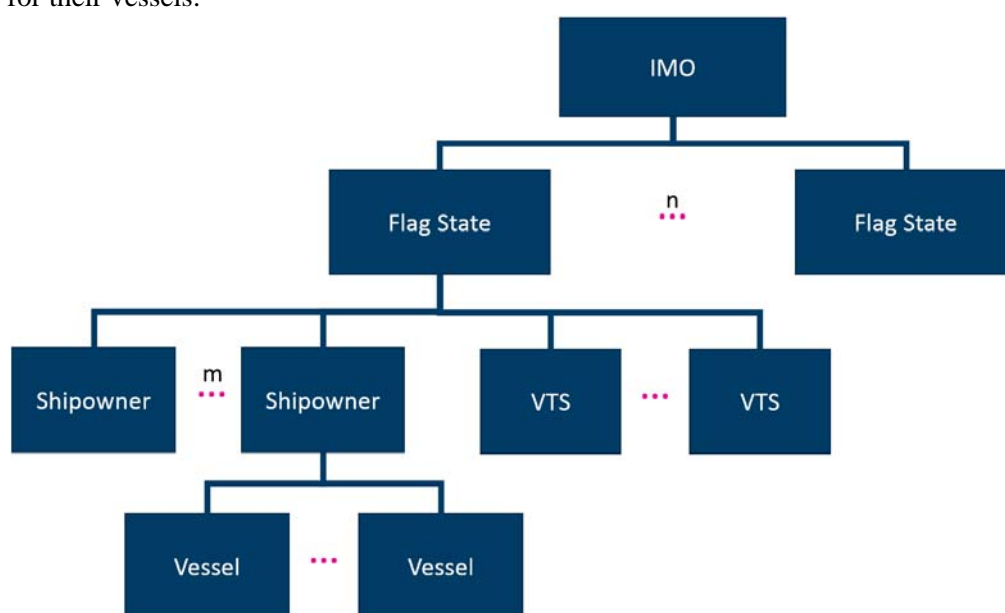
<sup>17</sup> Assumes full CRL distribution once a week. Optimisations like distributing new CRLs only when in port and otherwise relying on delta CRLs would significantly reduce the worst-case scenario. Depending on how common revocations are, it could be possible to have a CRL be valid for up to a year and only issue delta CRLs as needed

## 4 Alternative PKI hierarchies

In this section, we describe a number of different deployment alternatives for the Public Key Infrastructure (PKI) hierarchy. *Note that these are only examples; one can easily propose a number of other potential hierarchies.*

### 4.1 Alternative 1: IMO as root CA, Flag States and Shipowners as vertical intermediate CAs

In the first version, illustrated in Figure 16, IMO, as a trusted international organisation, will operate as the root CA and issue intermediate CA certificates for the individual Flag States, which will then be responsible for signing and revoking certificates for the VTS. The Flag States will also be responsible for issuing intermediate CA certificates for the shipowners, which in turn will be responsible for signing and revoking certificates for their vessels.



**Figure 16 PKI deployment - IMO operates as the as root CA and the Flag States operates as intermediate CAs. The shipowners are intermediate CAs for their vessels**

#### Pros

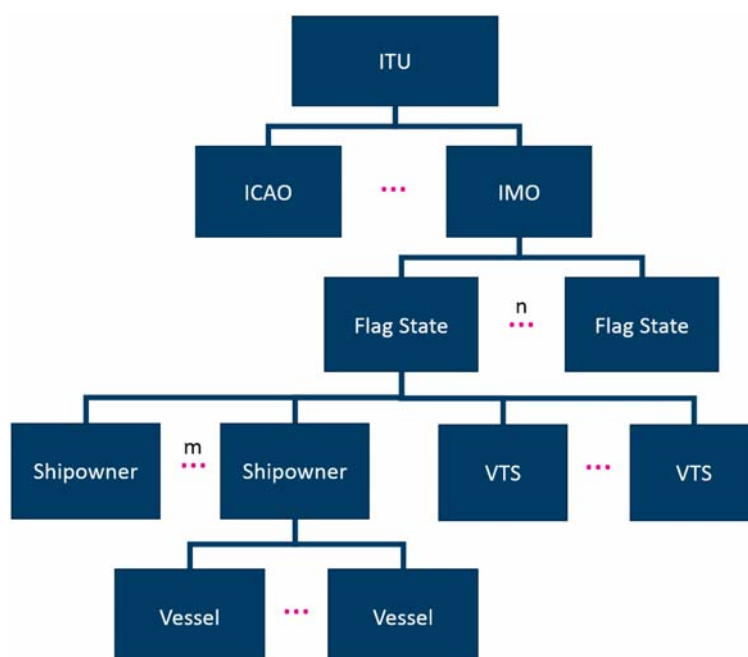
- Allowing Flag States to sign certificates for both shipowners and shore stations (VTS) means less administrative overhead for IMO
- Allowing shipowners to sign certificates for their own vessels means less administrative overhead for the Flag States

#### Cons

- Long certificates chains, which will require increased network capacity.
- Not possible to associate individual trust levels to different Flag States
- Not all shipowners may have the necessary technical competence needed to operate an intermediate CA
- A single root of trust represents a vulnerability in itself; compromising the root CA will compromise the whole PKI system

## 4.2 Alternative 2: ITU as root CA, IMO and ICAO as intermediate CAs

In the second version, illustrated in Figure 17, ITU operates as the root CA and IMO and ICAO are intermediate CAs. Apart from this, the PKI hierarchy is similar to the previous version (Figure 16 and share the same pros and cons. However, letting ITU take the role as the trusted root may simplify a future integration of the maritime and aviation communication infrastructures (i.e. for Search and Rescue operations).



**Figure 17: PKI deployment - ITU operates as root CA, ICAO and IMO operate as intermediate CAs and the Flag States operate as sub-CAs to IMO**

### Pros

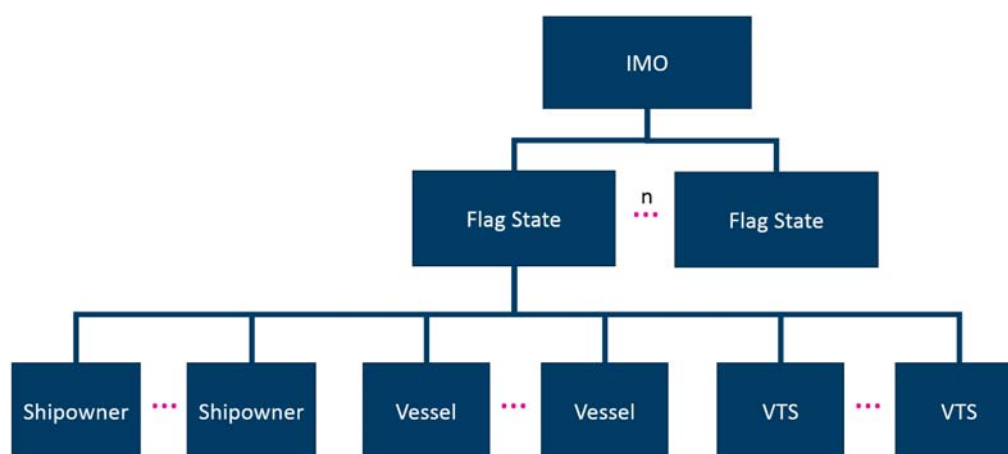
- Allowing Flag States to sign certificates for both shipowners and shore stations (VTS) means less administrative overhead for IMO
- Allowing shipowners to sign certificates for their own vessels means less administrative overhead for the Flag States

### Cons

- Very long certificates chains, which will require increased network capacity.
- Not possible to associate individual trust levels to different Flag States
- Not all shipowners may have the necessary technical competence needed to operate an intermediate CA
- A single root of trust represents a vulnerability in itself; compromising the root CA will compromise the whole PKI system

## 4.3 Alternative 3: IMO as root CA, Flag States as intermediate CAs

In the third version, illustrated in Figure 18, IMO operates as the as root CA and the Flag States operate as intermediate CAs. This is similar to the trust hierarchy in the first and second version; however, here the Flag States are intermediate CAs for shipowners, in addition to the vessels and VTS. The pros and cons are similar to the first case, with the exception that the shipowners do not have to operate their own CA.



**Figure 18: PKI deployment - IMO operates as the as root CA and the Flag States operates as intermediate CAs. The Flag States are intermediate CAs for shipowners, vessels and VTS**

#### Pros

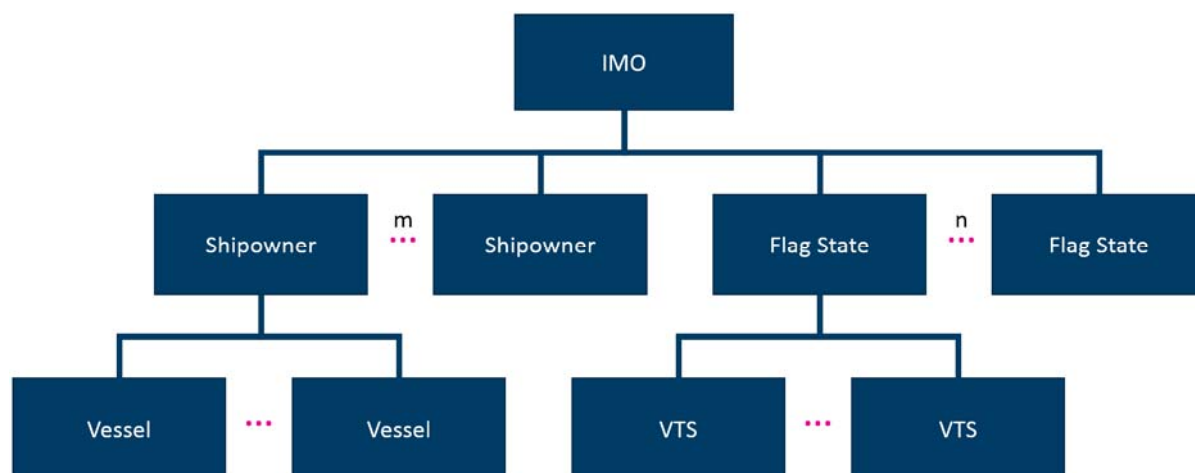
- Allowing Flag States to sign certificates for shipowners, vessels and shore stations (VTS) means less administrative overhead for IMO
- Short certificate chain

#### Cons

- More administrative overhead for the Flag States (signing vessel, shipowner and VTS certificates)
- Not possible to associate individual trust levels to different Flag States
- A single root of trust represent a vulnerability in itself; compromising the root CA will compromise the whole PKI system

### 4.4 Alternative 4: IMO as root CA, Shipowners and Flag States as horizontal intermediate CAs

In the fourth version, illustrated in Figure 19, both the Flag States and the shipowners operate their own intermediate CA. This option means less administrative overhead for the Flag States than the previous version, however, the burden on IMO will now increase.



**Figure 19: PKI deployment - IMO operates as root CA and the shipowners and Flag States operate as intermediate CAs**

#### Pros

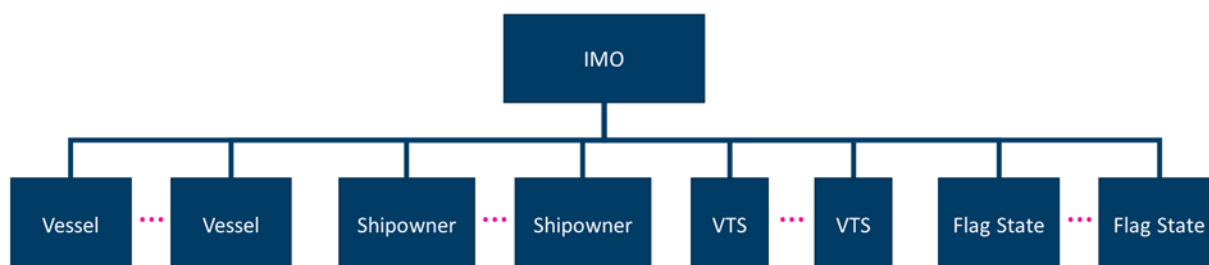
- Less responsibility for Flag States, which only needs to sign certificates for their shore stations (VTS)
- Short certificate chain

#### Cons

- Not possible to associate individual trust levels to different Flag States
- Not all shipowners may have the necessary technical competence needed to operate an intermediate CA
- A single root of trust represent a vulnerability in itself; compromising the root CA will compromise the whole PKI system

### 4.5 Alternative 5: IMO as root CA in a flat hierarchy

In the fifth version in Figure 20, IMO operates as the root CA in a flat hierarchy, i.e. there are no intermediate CAs. This solution is similar to the current implementation of the Maritime Cloud identity platform (where the Maritime Cloud operates as the root CA).



**Figure 20: PKI deployment - IMO operating as root CA, without any intermediate CAs.**

#### Pros

- Easy to set up and deploy
- A single organisation (IMO) is responsible

#### Cons

- Not possible to associate individual trust levels to different Flag States

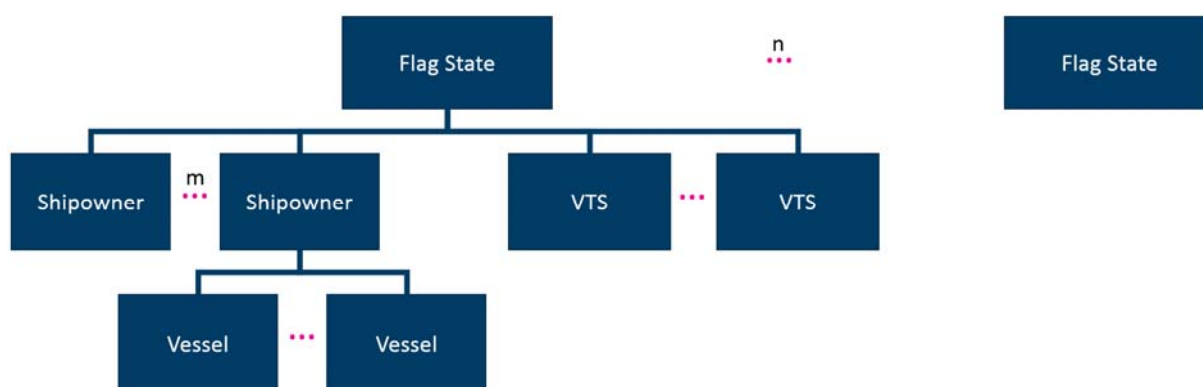


- for signing all the certificates
- Very short certificate chain

- Heavy administrative overhead for the organisation (IMO) operating the root CA
- A single root of trust represent a vulnerability in itself; compromising the root CA will compromise the whole PKI system

## 4.6 Alternative 6: Flag States operate their own root CAs

In the sixth version in Figure 21, each flag state will operate their own CA without a single root to connect them. This is similar to the ePassport approach presented in section 2.4.2.2.



**Figure 21: PKI deployment - Individual Flag States operate their own root CA**

### Pros

- No single root of trust could lead to a more robust solution
- Possible to assign individual trust level between different flag states
- Short certificate chain

### Cons

- All Flag States need to operate their own root CA, which will require strong security knowledge internally in all the organisations
- The Flag State need to agree on a solution for solving the key distribution problem<sup>18</sup>
- The number of root CA certificates that need to be distributed to the end entities will increase
- The risk of a compromised root CA will increase when there are so many root CAs

## 4.7 Certificate chain lengths and number of CRLs

Table 9 contains an overview over the number of certificates that will be included in the certification chains ("certificate chain length") and the number of CRLs that must be maintained in the different PKI

<sup>18</sup> For e-passports, this problem is solved by offering two different means to access root certificates from foreign countries; through bilateral means (diplomatic channels) or through an electronic exchange (ICAO Public Key directory or "master lists").

architectures presented in Section 4.1-4.6. In the table,  $n$  represents the number of Flag States and  $m$  represents the number of ship owners.

Alternative	Certificate Chain Length	Number of CRLs	Certificate Bundle Size <sup>19</sup>
1 (see Section 4.1)	4	$1 + (n \times m)$	4289 bytes
2 (see Section 4.2)	5	$1 + 2 + (n \times m)$	5396 bytes
3 (see Section 4.3)	3	$1 + n$	3182 bytes
4 (see Section 4.4)	3	$1 + n + m$	3182 bytes
5 (see Section 4.5)	2	1	2075 bytes
6 (see Section 4.6)	3	$n \times m$	3182 bytes

**Table 9 Certificate chain length and number of CRLs for the different PKI hierarchy alternatives presented in this chapter**

<sup>19</sup> Worst case while assuming ECC keys of 384 bit length and X.509 certificates for all participants. This number also assumes an offline root CA. If an online intermediate CA is to be used at the root level, each value must be increased by 1107 bytes. The used curve is secp384r1 on OpenSSL

## 5 Evaluation of alternatives with respect to the design goals

This section evaluates the proposed PKI properties in Section 3 and the alternative PKI hierarchies in Section 4 with respect to the design goals that we formulated in Section 2.3.

The ✓ symbol indicates that the design goal can be fulfilled. The X symbol indicates that the goal cannot be fulfilled. A question mark indicates that, in this point in time, we cannot say for sure whether the goal can be fulfilled or not. In some of the boxes, we have used text to further explain the conclusions that we have made.

The "n/a" indicates that the design goal is irrelevant for the evaluated functionality. For example, the future service applicability of the PKI solution (design goal 5) is not relevant when discussing where to store the private keys and root certificates, or how to do the enrolment of the certificates to the vessels.

The shaded boxes represent solutions that have not been described in this document. For example, we have not proposed a solution in which the PKI functionality is embedded in VDES software, without utilizing smartcards or HSMs.

Design goal	VDES			Dedicated PKI unit			Bridge computer		
	Smartcards	HSMs	Software	Smartcards	HSMs	Software	Smartcards	HSMs	Software
1	✓			✓	✓	✓	✓	✓	✓
2	✓			✓	✓	✓	✓	✓	✓
3	✓			✓	✓	✓	✓	✓	✓
4	✓	✓		✓	✓	✓	✓	✓	✓
5	✓			✓	✓	✓	✓	✓	✓
6	n/a	n/a		n/a	n/a	n/a	n/a	n/a	n/a
7	n/a	n/a		n/a	n/a	n/a	n/a	n/a	n/a
8	n/a	n/a		n/a	n/a	n/a	n/a	n/a	n/a
9	✓	✓		X Introducing new HW means an increased cost		✓	✓	✓	✓
10	n/a	n/a		n/a	n/a	n/a	n/a	n/a	n/a
11	n/a	n/a		n/a	n/a	n/a	n/a	n/a	n/a
12	n/a	n/a		n/a	n/a	n/a	n/a	n/a	n/a
13	✓	✓		✓	✓	X Software alone does not offer secure storage	✓	✓	X Software alone does not offer secure storage
14	✓	An HSM		✓	An HSM	✓	✓	An HSM	✓

	VDES			Dedicated PKI unit			Bridge computer		
	Smartcards	HSMs	Software	Smartcards	HSMs	Software	Smartcards	HSMs	Software
		is difficult to upgrade			is difficult to upgrade			is difficult to upgrade	

**Table 10 An evaluation of the PKI storage and processing units alternatives for the vessels**

Design goal	VDES			Dedicated PKI unit			Bridge computer		
	Smartcards	HSMs	Software	Smartcards	HSMs	Software	Smartcards	HSMs	Software
1	n/a	n/a		n/a	n/a				n/a
2	n/a	n/a		n/a	n/a				n/a
3	n/a	n/a		n/a	n/a				n/a
4	n/a	n/a		n/a	n/a				n/a
5	n/a	n/a		n/a	n/a				n/a
6	✓ Only the CSRs (or activation codes) and the signed certificates need to be delivered over the air.  Note that alt 5 is an offline enrolment solution			✓ Only the CSRs (or activation codes) and the signed certificates need to be delivered over the air.	✓ Only the CSRs (or activation codes) and the signed certificates need to be delivered over the air.				✓ Only the CSRs (or activation codes) and the signed certificates need to be delivered over the air.
7	✓ In alt 1-5 the shipping company needs to handle the enrolment  In alt 2 & 4 the crew also needs to be involved  Alt. 6 requires no involvement by shipping company or crew	✓ In alt 9 the shipping company needs to handle the enrolment		✓ In alt 13 the shipping company needs to handle the enrolment	✓ In alt 11 the shipping company needs to handle the enrolment				X High technical competence required in the shipping companies.
8	n/a	n/a		n/a	n/a				n/a
9	? Enrolment costs have not been assessed	? Enrolment costs have not been assessed		? Enrolment costs have not been assessed	? Enrolment costs have not been assessed				? Enrolment costs have not been assessed (however

	VDES			Dedicated PKI unit			Bridge computer		
	Smartcards	HSMs	Software	Smartcards	HSMs	Software	Smartcards	HSMs	Software
									few actors involved means less cost)
10	n/a	n/a		n/a	n/a				n/a
11	n/a	n/a		n/a	n/a				n/a
12	✓	✓		✓	✓				✓
	Note that alt 2 requires advanced logistics								
13	✓	✓		✓	✓				Less secure storage of keys and root CA certificate  Note that alt 7 does not use pre-generated key pairs
	Note that alt 1 does not use pre-generated key pairs and alt 4 makes it possible for an attacker to obtain a valid activation code	Note that alt 9 does not use pre-generated key pairs			Note that alt 11 does not use pre-generated key pairs				
14	n/a	n/a		n/a	n/a				n/a

**Table 11 An evaluation of the PKI certificate enrolment alternatives for the vessels**

Design goal	CRL	Eventually consistent CRL	OCSP	Stapled OCSP	Stapled OCSP + CRL
1	n/a	n/a	n/a	n/a	n/a
2	n/a	n/a	n/a	n/a	n/a
3	n/a	n/a	n/a	n/a	n/a
4	✓	✓	Requires constant connectivity in order to validate certificates	Given a long enough lifetime on the Stapled OCSP signatures, this solution will work offline. However, there is a need of being online at given intervals to obtain a new stapled OCSP	✓
5	n/a	n/a	n/a	n/a	n/a
6	This would depend on the configuration of the system. If CRLs have a short lifetime, it would require large amounts of bandwidth. If CRLs are given a longer lifetime, the bandwidth use will be reduced	Will require less centralised bandwidth and vessels will be able to obtain the needed CRLs on demand. This will reduce the bandwidth needs	If each vessel only ever communicates with a low number of other actors, the bandwidth consumption will be quite low. If each actor communicates with a larger amount of actors, the bandwidth consumption will be comparable or larger than the CRL	The amount of requests for certificate validation will be limited by the number of issued certificates	See the columns for CRL and Stapled OCSP
7	This will depend on the chosen PKI hierarchy	This will depend on the chosen PKI hierarchy and the trust placed in	This will depend on the chosen PKI hierarchy	This will depend on the chosen PKI hierarchy	This will depend on the chosen

Design goal	CRL	Eventually consistent CRL	OCSF	Stapled OCSF	Stapled OCSF + CRL
8		that another vessel will provide the newest CRL received rather than an old one			PKI hierarchy
9	n/a	n/a	n/a	n/a	n/a
10	This will depend on the chosen PKI hierarchy, the lifetime of the CRL, and the amount of revocations	Probably less expensive than regular CRLs with regard to bandwidth, but increased complexity also brings a cost	Expensive through not working offline and being vulnerable to simple DoS-attacks	Low bandwidth cost per vessel	This will depend on the chosen PKI hierarchy, the lifetime of the CRL, and the amount of revocations
11	n/a	n/a	n/a	n/a	n/a
12	✓	✓	✓	✓	✓
13	n/a	n/a	n/a	n/a	n/a
14	n/a	n/a	n/a	n/a	n/a

**Table 12 An evaluation of the PKI certificate revocation alternatives for the vessels**

Design goal	Alt 1: IMO as root CA, Flag States and Shipowners as verificational intermediate CAs	Alt 2: ITU as root CA, IMO and ICAO as intermediate CAs	Alt 3: IMO as root CA, Flag States as intermediate CAs	Alt 4: IMO as root CA, Shipowners and Flag States as Horizontal intermediate CAs	Alt 5: IMO as root CA in a flat hierarchy	Alt 6: Flag States operate their own root CAs
1	✓	✓	✓	✓	✓	✓
2	n/a	n/a	n/a	n/a	n/a	n/a
3	n/a	n/a	n/a	n/a	n/a	n/a
4	n/a	n/a	n/a	n/a	n/a	n/a
5	✓	✓ ITU as the root of trust could simplify future communication with other domains, such as aviation	✓	✓	✓	✓
6	Long certificate chains requires more bandwidth	Long certificate chains requires more bandwidth	✓	✓	✓	Numerous CRLs need to be maintained by the vessels
7	Shipowners need to be able to their own intermediate CA	Shipowners need to be able to operate their own intermediate CA.  ITU will need to operate a world-wide root CA for maritime	Flag States will be responsible for individual vessel certificates	Shipowners need to be able to operate their own intermediate CA	IMO's responsibilities will increase heavily	Shipowners need to be able to operate their own intermediate CA
8	✓	✓ ITU as the root of	✓	✓	✓	✓

9		trust could simplify future communication with other domains				
	Two intermediate CAs means more costs	Three intermediate CAs means more costs	✓	✓	✓	✓
	n/a	n/a	n/a	n/a	n/a	n/a
	n/a	n/a	n/a	n/a	n/a	n/a
	✓	✓	✓	✓	A flat hierarchy is not feasible to deploy on a global basis	A global solution with individual Flag State CAs may be cumbersome to deploy
13	n/a	n/a	n/a	n/a	n/a	n/a
14	n/a	n/a	n/a	n/a	n/a	n/a

**Table 13 An evaluation of the PKI hierarchy alternatives**

The results in Table 10 - 13 will be used as input to deliverable D2.2 when make a decision on how to deploy and operate the PKI.



## 6 Summary and future work

This deliverable has explored the available possibilities with regard to certificates, cryptographic strength, practical options on how to add the solution to vessels, enrolment options, rekeying, revocation, and finally some potential PKI hierarchies.

The deliverable has been based on a preliminary set of use cases (Section 2.3) and an early draft of the VDES standard, and thus it is too early to provide an exact recommendation of solutions at this time – even though a preliminary evaluation has been conducted.

Consequently, deliverable D2.2 will address the following aspects:

- The exact usage of the solution based on an extended evaluation of the modified and new use cases
- Evaluation of the potential solutions based on the expected usage, constraints from communication channels, and requirements from the risk assessment in deliverable D1.1
- Selection of solution and detailed design
- Procedures for operating the PKI
- Detailed operations for ship-to-ship, ship-to-shore, shore-to-ship, and shore-to-shore

For the solution to be adopted by the worldwide maritime community it needs to be standardized. As mentioned in Section 2.4.1, 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.

The results from work package H2 is intended to be used as input to a standards process. An extended abstract of the D2.1 and D2.2 documents will therefore be compiled and sent to IMO, IALA, Sjøfartsdirektoratet and Kystverket for feedback, and will be used as input to further discussions on security solutions for international maritime communication.

## 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](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] R. Shirey, "RFC 4949 - Internet Security Glossary, Version 2," *IETF*, 2007. [Online]. Available: <https://tools.ietf.org/html/rfc4949>. [Accessed: 01-Jan-2001].
- [6] D. A. Nesheim, Ø. Rødseth, and P. H. Meland, "D1.1a Context and user requirements," 2016.
- [7] IMO, "GUIDELINES ON THE FACILITATION ASPECTS OF PROTECTING THE MARITIME TRANSPORT NETWORK FROM CYBERTHREATS - The Guidelines on Cyber Security onboard Ships," 2015.
- [8] ISO, "Future Proof and Cost-Effective Standardization of Electronic Ship Certificates," 2015.
- [9] H. Peiponen and A. Kukkonen, "Integrity monitoring and authentication for VDES Pre-Distributed Public Keys," 2010.
- [10] IMO, "LONG-RANGE IDENTIFICATION AND TRACKING SYSTEM TECHNICAL DOCUMENTATION (PART I)," 2014.
- [11] IMO, "LONG-RANGE IDENTIFICATION AND TRACKING SYSTEM TECHNICAL DOCUMENTATION (PART II)," 2014.
- [12] European Maritime Safety Agency (EMSA), "Annex 3 LRIT International Data Exchange ( IDE ) Functions and Architecture," 2013.
- [13] EMSA, "ANNEX III Security Guidelines SafeSeaNet," 2013.
- [14] International Hydrographic Organisation, "IHO Data Protection Scheme Edition 1.1.1," 2012.
- [15] EfficienSea, "Deliverable 3.1. Analysis Report. Maritime communication and infrastructure Analysis," 2015.
- [16] EfficienSea, "Deliverable 3.2. Conceptual Model," 2016.
- [17] "Technical Guideline TR-03110-3. Advanced Security Mechanisms for Machine Readable Travel Documents," 2015.
- [18] Frontex, "Operational and Technical security of Electronic Passports," 2011.
- [19] Inmarsat, "Iris Precursor Phase 1- Final Report," 2015.
- [20] 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].
- [21] P. Yee, "RFC 6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2013. [Online]. Available: <https://tools.ietf.org/html/rfc6818>. [Accessed: 06-Sep-2016].
- [22] "RSA Laboratories. PKCS #1: RSA Cryptography Standard." [Online]. Available: <http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-rsa-cryptography-standard.htm>.

- [23] "RSA Laboratories. 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>.
- [24] ENISA, "Algorithms, key size and parameters report - 2014," 2014.
- [25] 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](http://web.archive.org/web/20090117023500/http://www.nsa.gov/business/programs/elliptic_curve.shtml). [Accessed: 06-Sep-2016].
- [26] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post - Quantum Cryptography Report on Post - Quantum Cryptography," 2016.
- [27] W. Vogels, "Eventually Consistent," *Communications of the ACM - Rural engineering development*, pp. 40–44, 2009.
- [28] 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].
- [29] 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].
- [30] D. Eastlake, "RFC 6066 - Transport Layer Security (TLS) Extensions: Extension Definitions," *IETF*, 2011. [Online]. Available: <https://tools.ietf.org/rfc/rfc6066.txt>. [Accessed: 20-Sep-2016].
- [31] Danish Maritime Authority, "Identity Management In The Maritime Cloud."

## A Abbreviations and glossary

AIS	Automatic Identification System
ASM	Application Specific Messages
ASP	Application Service Provider
ATM	Air Traffic Management
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 certificates and certificate revocation lists (CRLs) on request to any entity in the system
CN	Common Name
Costal 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
CSCA	Country Signing Certification Authority
CVC	Card Verification Code
CySiMS	Cyber Security in Merchant Shipping
DMA	Danish Maritime Authority
DS	Document Signer
DVCA	Document Verifier Certification Authority
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithmic Problem
e-MRTD	Electronic Machine Readable Travel Documents
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
Eventually consistent	A distributed system is said to be eventually consistent if it operates in such a way that if no new data is introduced into the system, all nodes will eventually converge to hold the same data
Flag State	The nation which guarantees for the state and compliance with international regulations of the vessel
GISIS	Global Integrated Shipping Information System
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
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 certificates to child CAs
IS	Information System
Issuing CA	Subordinate CA issuing 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 Certificate	A digital certificate attesting to the identity of the holder and can be used in cryptographic functions
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 vessel in question
RA	Registration Authority
Revocation	The process of withdrawing a previously signed PKI Certificate
RO	Recognised Organisation
RSA	Rivest, Shamir, and Adleman. Cryptographic algorithm
SAR	Search and Rescue
SAS	Satellite Anchor Station
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 PKI Certificate. The value is verifiable by means of the PKI 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



Technology for a better society

[www.sintef.no](http://www.sintef.no)