SINTEF

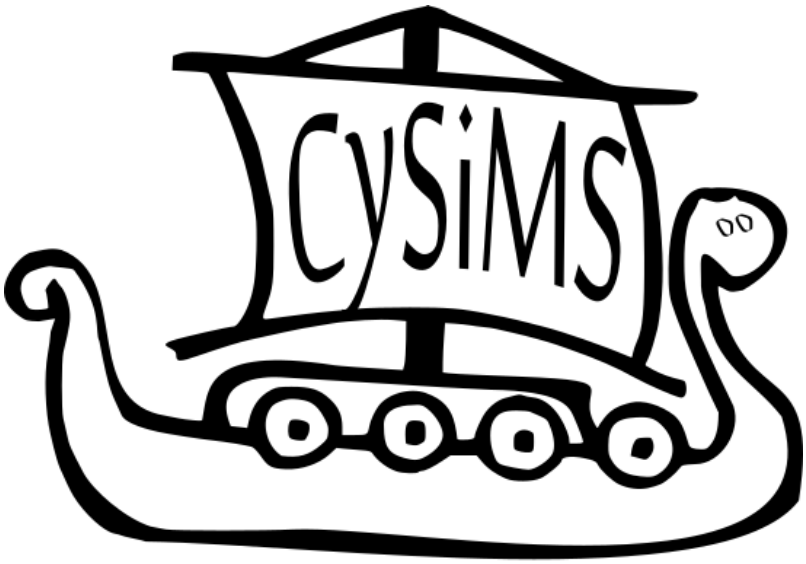
2021:00314- Unrestricted

CySiMS-SE deliverable

D4.3 Multi-modal communication

Securing future communication across different sectors and technologies

Authors
Karin Bernsmed
Guillaume Bour
Per Håkon Meland
Ravi Borgaonkar
Egil Wille



KONGSBERG SINTEF NAVTOR KYSTVERKET The Research Council of Norway

SINTEF Digital
SINTEF Digital
Address:

NO-
NORWAY
Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

CySiMS-SE

D4.3 Multi-modal communication

Securing future communication across different sectors and technologies

KEYWORDS:
Cyber security, maritime, PKI, VDES, information exchange, Search and Rescue

VERSION	DATE
1.0	2021-03-25

AUTHOR(S)
Karin Bernsmed
Guillaume Bour
Per Håkon Meland
Ravi Borgaonkar
Egil Wille

CLIENT(S)	CLIENT'S REF.
The Research Council of Norway	CySiMS SE (295969)

PROJECT NO.	NUMBER OF PAGES/APPENDICES:
102019295	10

ABSTRACT
This document introduces the concept of multi-modal communication, using the coordination of a Search and Rescue (SAR) operation as an illustrating scenario, identifies challenges for secure information exchange and outlines the way forward.

PREPARED BY	SIGNATURE
Karin Bernsmed	

CHECKED BY	SIGNATURE
Dag Atle Nesheim	

APPROVED BY	SIGNATURE
Maria Bartnes	

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
2021:00314	978-82-14-06462-9	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2021-03-16	First complete version sent to internal review
0.2	2021-03-17	Second complete version sent to internal review
1.0	2021-03-25	Final version

Table of contents

Abbreviations

In this document, the following abbreviations have been used:

AIS	Automatic Identification System
AtoN	Aids to Navigation
BB	Bulletin Board
CA	Certificate Authority
CySiMS	Cyber Security in Merchant Shipping
CySiMS-SE	CySiMS Service Evolution
EU	European Union
IMO	International Maritime Organization
MRCC	Maritime Rescue Coordination Centre
MRN	Maritime Resource Name
PKI	Public Key Infrastructure
SAR	Search and Rescue
SART	Search and Rescue Transceiver
VDE	VHF Data Exchange
VDES	VHF Data Exchange System
VDES-SAT	The satellite component of VDES
VDES-TER	The terrestrial component of VDES
VHF	Very High Frequency
VTS	Vessel Traffic Service

1 Introduction

The maritime sector and infrastructure are critical to Norway, EU and the world economy. Digital technology for ships is in continuous development, and cyber security is an important enabler to ensure safe and reliable operations. Cyber Security in Merchant Shipping (CySiMS) (2015-2018) was a Research Council of Norway funded project, which designed security solutions to protect digital communication in the maritime domain. The results have been met with much interest in the maritime community, but there is now an urgent need to develop the specifications from the CySiMS project into a complete system.

The underlying idea of CySiMS-SE is to demonstrate and operationalize a secure communication solution for the maritime sector and integrating this with the onboard computer architecture. The solution will include a Public Key Infrastructure (PKI) and necessary hardware and software for secure information exchange across systems on the bridge, off-bridge and on shore. This will provide a world's first open, integrated, and cost-effective protection against cyber-attacks on critical safety and operational information, while contributing to preserving Norway's position as a seafarer nation leading the way in developing, adopting and selling technological innovations.

The "CySiMS PKI" (described in [1], [2] and [3]) has been designed for application in the maritime domain, where ship-and shore-side actors communicate over the upcoming VHF Data Exchange System (VDES). However, challenges may arise when communication between stakeholder across sectors may be needed, and/or where different communication channels are utilized. In this document we use coordination of search and rescue operations as an example of such scenario, and we outline and discussed the challenges that need to be solved.

2 Multimodal communication

By *multimodal communication*, we mean communication that uses several means of communication technology, either in parallel at the same time or through a link of serial connections. This could be communicating using different types of networks, and/or transmission technologies. For instance, a Vessel Traffic Service (VTS) that monitors ships in its adjacent area using AIS received both from ordinary AIS base stations and from the terrestrial component of VDES (VDES-TER) and the satellite components of VDES (VDES-SAT).

Mixing communication technologies often requires actors from different sectors or domains to collaborate to get the information to its destination, hence *cross-domain* communication is closely related to multimodal communication. An example could be a maritime traffic tracking service that provides position data from ships to a port logistics platform, which uses it to coordinate ground-based transport.

The CySiMS PKI has been designed to allow actors in the maritime domain to identify and authenticate each other, to authenticate and check the integrity of the messages that they send to each other, and to establish secure channels for communication. These actors can be any type of ship- or shore-side entities. Examples are ships, VTS stations and future e-navigation services.

For the representation of the *identities* of these actors, the CySiMS PKI utilizes the Maritime Resource Name (MRN) [4], which is a naming scheme that can uniquely identify any maritime resource on a global scale. This naming scheme including all kinds of maritime resources that has an identity of some kind. Resources from other sectors are hence not included here.

The CySiMS PKI has been designed for application layer communication over VDES. It may also be used to authenticate the Bulletin Board (BB) messages of the VDES, provided that the allocated slot for digital signature in the BB will be long enough[1].

It is expected that AIS infrastructure both on the shore- and shipside will be upgraded with VDES capabilities over the next 5 to 10 years, by replacing existing AIS ship equipment with combined AIS and VDES terminals [5].

3 Example: Coordination of a Search and Rescue (SAR) operation

Figure 1 outlines a scenario where a man overboard, who is wearing a Search and Rescue Transceiver (SART) device, is located by nearby ships, a Search and Rescue (SAR) aircraft, and a SAR helicopter. The search and rescue operation is coordinated by a Maritime Resource Coordination Centre (MRCC), which exchanges search coordination data and search patterns with the involved actors (ships, helicopter, and aircraft) using the network connectivity provided by the VDES ground (VDES-TER) and VDES space (VDES-SAT) segments. The MRCC also collects "ordinary" AIS data from ships in the nearby area and metrology data about the current sea conditions from an AtoN beacon. In this scenario, the rescue process can be streamlined by means such as, better and more efficient communication with the involved actors, visualization of the search patterns on an electronic map, etc [5][6]. Depending on circumstances, the MRCC may also need to exchange information with other stakeholders, such as the coastguard, the police, the red-cross, the armed forces, medical communication centres and hospitals [7].

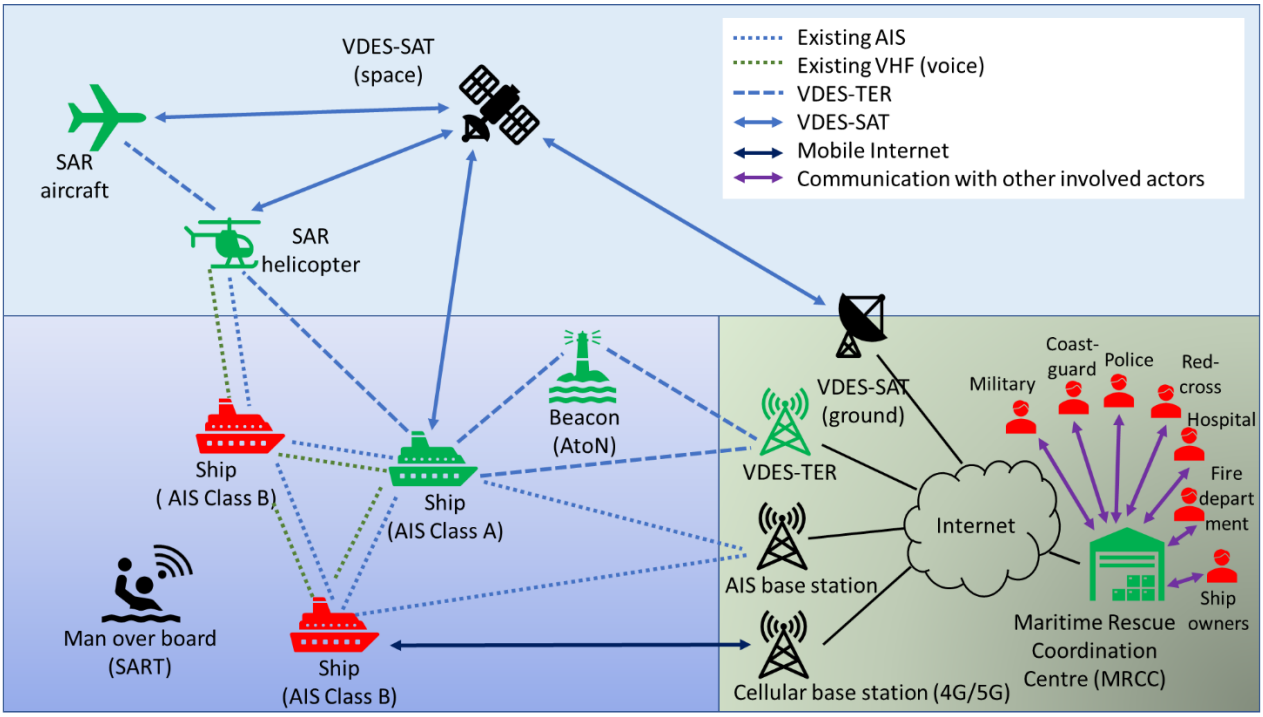


Figure 1 Digital communication infrastructure used for future coordination of search and rescue (SAR) operations. Actors/entities that can (or cannot) be enrolled in the CySiMS PKI are marked with green (or red, respectively).

[1] VDES is currently being standardized and, at the time of writing, the allocated length for the signature field of the BB has not been decided upon.

4 Secure multi-modal communication

The CySiMS PKI can "enable" security in a scenario like the one outlined in Figure 1, by providing authenticity and integrity protection of the information that is exchanged and by allowing the communicating actors to establish a secure link for the exchange of information. Those actors are marked with green in the figure. Enabling security means that the actors can make sure that no unauthorised persons and/or organisations are interceptions and/or disturbing the communication[2]. However, one needs to make sure that also:

- Actors with outdated technology, for example a nearby leisure ship with "old fashioned" AIS equipment (Class B, marked with red in the figure), must be able to send and receive relevant information, but by using the existing AIS and VHF (voice) communication channels.
- Actors without VDES connectivity, for example a nearby ship with a mobile Internet connection (also marked with red in the figure), must be able to send and receive relevant information, but by using their existing network connection.
- Actors from other sectors, such as the coastguards, the police, the red-cross, etc (also marked by red in the figure), must be able to collaborate and exchange relevant information.

Ideally, a security solution should be able to function properly also under such circumstances, thereby providing a holistic way of securing communication in multi-modal and cross-domain scenarios. To achieve this goal, we foresee the following possible way forward:

A. All actors are enrolled in the same (maritime) PKI, managed by the same Certificate Authority (CA). If there are several PKIs for each domain, entities can have multiple certificates (one for each for PKI).
B. Establishing trust between the CAs of the different domains. Each CA manages its own “forest” of entities. It is possible to use cross-forest enrolment to issue certificates to entities in one forest from a CA in another forest (see [8], page 30). Cryptographic protocols, algorithms and key lengths must be compatible.
C. Establishing trust between the CAs of the different domains using Blockchain [9]. A Blockchain, by definition, can create trust where there is none, and could thus be used to allow secure cross domain communication. This solution is less mature than the cross-forest enrolment (proposed in B), but would allow the use of different cryptographic protocols, algorithms, and key lengths.
D. Fallback to an insecure channel for a short period of time. For example, in an emergency, actors can choose to ignore signature and/or disable encryption. After such event, there should be a thorough post-event analysis looking for possible misuse of the system.
E. When messages are relayed through different sectors, using different communication technologies, use wrapping/tunnelling to protect the information where possible.
F. When messages are relayed through different sectors, using different communication technologies and different message formatting (e.g., data - voice), rely on point-to-point security solutions.

Future research should hence:

- Determine the requirements for a cross domain solution for secure communication. Different sectors have different requirements, different standards, and different challenges. This should involve the stakeholders/actors from the different sectors.
- Review existing solutions and the possible new solutions and see whether/how they can fulfil the requirements from the different sectors.
- Design, implement, test, and evaluate potential solution(s) in a selected set of scenarios.

[2] In Search and Rescue (SAR) operations, failure of the communication equipment can have severe consequences. Researchers have raised concerns about the potential of cyber-attacks to cause physical disasters, or to maximize the impact of existing ones by intentionally disturbing and/or interfering with the coordination of the operation [10].

5 References

[1] Christian Frøystad, Karin Bernsmed, and Per Håkon Meland. 2017. Protecting Future Maritime Communication. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 97, 1–10. DOI: https://doi.org/10.1145/3098954.3103169

[2] CySiMS SE project deliverable. D4.1 PKI prototype specification. Version 1.2, April 2020.

[3] CySiMS SE project deliverable. D4.2 Onboard Cryptographic Unit specifications - PKI Unit for security services in the maritime sector. Version 1.0, April 2020.

[4] Maritime Resource Name registry. https://www.iala-aism.org/technical/data-modelling/mrn/

[5] https://spacenorway.no/vhf-data-exchange-system-vdes-page-under-development/

[6] https://business.esa.int/projects/jericho-vde

[7] Andreassen, N., Borch, O. J., & Sydnes, A. K. (2020). Information sharing and emergency response coordination. Safety Science, 130, 104895.

[8] Internet X.509 Public Key Infrastructure: Certification Path Building. RFC4158, Sep 2005. https://tools.ietf.org/html/rfc4158

[9] Rødseth, Ø. J., Meland, P. H., Frøystad, C., & Drugan, O. V. (2019). PKI vs. Blockchain when Securing Maritime Operations.

[10] Loukas, George & Gan, Diane & Vuong, Tuan. (2013). A Review of Cyber Threats and Defence Approaches in Emergency Management. Future Internet. 5. 205-236. 10.3390/fi5020205.