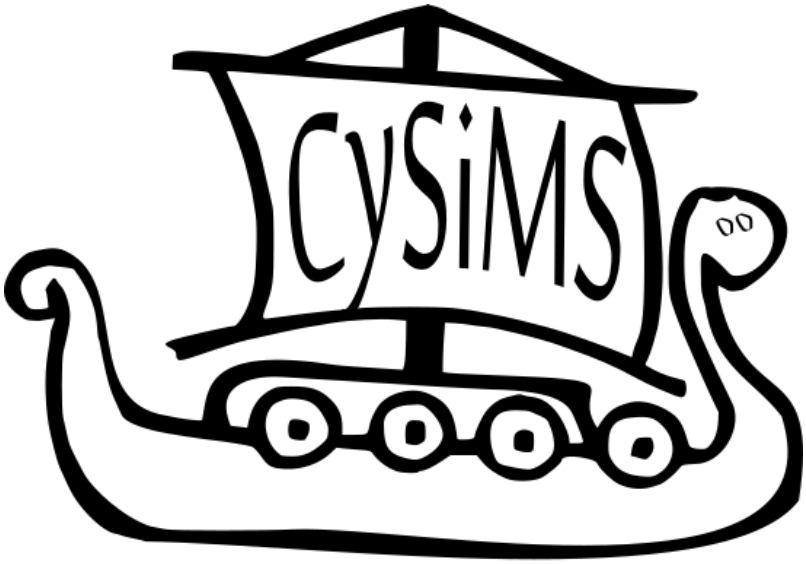
SINTEF

2021:00319- Unrestricted

# CySiMS-SE deliverable

## D2.3 CySiMS Cyber Event Exercise Handbook

**Authors**
Karin Bernsmed
Ravi Borgaonkar




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

# D2.3 CySiMS Cyber Event Exercise Handbook

KEYWORDS:
Cyber security, maritime, PKI, VDES, exercise

| | | | |
|---|---|---|---|
| **VERSION**<br>1.1 | | | **DATE**<br>2021-03-23 |
| **AUTHOR(S)**<br>Karin Bernsmed<br>Ravi Borgaonkar | | | |
| **CLIENT(S)**<br>The Research Council of Norway | | | **CLIENT'S REF.**<br>CySiMS SE (295969) |
| **PROJECT NO.**<br>102019295 | | | **NUMBER OF PAGES/APPENDICES:**<br>14 |
| **ABSTRACT**<br>This document is a handbook for developing cyber event exercises relevant for the intended users of the CySiMS-SE secure communication solution. The document includes a selected set of scenarios that are relevant to prepare for, including both the enrolment of ships into the PKI and the use of the PKI to secure maritime communication. The document also provides two examples of exercises. | | | |
| **PREPARED BY**<br>Karin Bernsmed | | | SIGNATURE |
| **CHECKED BY**<br>Per Håkon Meland | | | SIGNATURE |
| **APPROVED BY**<br>Maria Bartnes | | | SIGNATURE |
| **REPORT NO.**<br>2021:00319 | **ISBN**<br>978-82-14-06463-6 | **CLASSIFICATION**<br>Unrestricted | **CLASSIFICATION THIS PAGE**<br>Unrestricted |

# Document history

| VERSION | DATE | VERSION DESCRIPTION |
|---|---|---|
| 1.0 | 2021-03-18 | First complete version |
| 1.1 | 2021.03.23 | Final version |

# Table of contents

# 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 onshore. This will provide the 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 leading seafarer nation leading the way in developing, adopting and selling technological innovations.

This document is a handbook for developing cyber event exercises that are relevant for the intended users of the CySiMS-SE secure communication solution. More specifically, the document includes a selected set of scenarios that are relevant to prepare for, for the end users who are involved in the enrolment of ships into the PKI or in the use of the PKI to secure maritime communication. We also provide two examples of how these scenarios can be turned into exercises.

# 2 Cyber event exercises

A cyber event exercise is used to practice on a scenario where one or more things deviate from expected behaviour, to be better prepared to handle such situations in the future. Performing a cyber event exercise includes planning, preparation, and execution of one or more scenarios, with the purpose of training, evaluation, and learning. Cyber event exercises can many take different forms. Full descriptions of the different types of exercises, including guidelines for planning and execution of the exercises, is thoroughly described in the "Cyber Exercise Playbook" from the MITRE Corporation [1] and the "NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" from the National Institute of Standards and Technology [2]. In this section we provide a brief introduction to the different types of exercises and how to plan, prepare and execute such exercises.

## 2.1 Types of exercises

The three most applied type of exercises are table-top exercises, full live exercises, and hybrid exercises.

**Table-top exercises** are discussion-based exercises where the participants sit down together, for example in a in a meeting room, to discuss their roles during a cyber event and their responses to the situation that they will be facing in the cyber event. The exercise is based around a scenario, which is introduced by a facilitator, who then initiates the discussion and asks the exercise participants questions that are related to the scenario and that are relevant for their roles. A table-top exercise is discussion-based only and does usually not require any equipment or other kind of resources [2]. An example of a relevant table-top exercise for the maritime industry, in the context of the CySiMS project, would be to gather relevant personnel from the supplier of the PKI-unit (Kongsberg Defence and Aerospace), from the operators of the PKI service (The Norwegian Maritime Authority - Sjøfartsdirektoratet) and from the ship owners, to discuss how to handle a situation where the Root CA private key has been compromised.

A table-top exercise should have a small training audience and a well-defined objective. The "injects" to the exercises are hypothetical, entirely pre-coordinated, and written down in advance when the exercise is planned. Table-top exercises are well suited for the participants to get familiarized with existing plans and

procedures in their organisations, communication structures and their ability to respond to the events that unfold during the exercise. This type of exercise is commonly used to establish relationships and share information within the organization and/or with its partners, to test the readiness of response capabilities, and to raise awareness on the need to prepare for cyber events [1][2].

**Full live exercises**, sometime referred to as functional exercises, or simulated exercises, are based on real events, in a real setting, with the purpose to increase the realisms of the scenario. Full live exercises are often performed in conjunction with "red teams"[1], which initiates real attacks against pre-defined targets. Full live exercises often include multiple organisations and require synchronisation within the organisations, since they may interfere with the organisations' day-to-day activities and their existing networks and services [1]. A full live exercise typically lasts from between several hours to several days, depending on the event's objectives and the complexity of the plan being exercised [2]. An example of a full live exercise for the maritime industry, in the context of the CySiMS project, would be to let a "red team" (for example, from SINTEF) to compile false navigational information and transmit it to the ships that are participating in the project live demonstrations.

A full live exercise often includes multiple organisations. Like a table-top exercise, the functional exercise is scenario-driven, and it is common to simulate multiple scenarios that arise during the exercise. Full live exercises are particularly suitable for allowing personnel with operational responsibilities to validate the organisations' incident management plans and their operational readiness for emergencies, by letting them perform their duties and responding to the situations that arise in the simulated scenarios [1].

**Hybrid exercises** are a are a mix between table-top and full live exercises, in which, for example, the discussions in the table-top exercise are enhanced by "injects" of simulated events. The intention is to increase the realism and training opportunities for the participants, while keeping the required resource and time needed for planning and execution of the exercise to an acceptable level.

The Cyber Exercise Playbook from the MITRE Corporation [1] provides a good overview and comparison of these three types of exercises, which we have reproduced in Table 1.

**Table 1 The characteristics of the different types of cyber event exercises (adapted from [1]).**

| Type | Description | Timing | Resources | Suitable for |
|---|---|---|---|---|
| **Table-top** | Paper-driven exercise with injects scripted by the exercise planners and delivered via paper (cards/ discussion) | Planning: 1–2 months | Table-top | Paper-driven exercise with injects scripted by the exercise planners and delivered via paper (cards/ discussion) |
| **Hybrid** | Paper driven exercise with injects of one or more live scenarios facilitated by a "Red Team"1 for realism | Planning: 3–6 months. Execution:3–5 days. | Requires more people and time, real targets for scenarios, deconfliction contacts | Organisations already familiar with (inter-organization) exercises. |

[1] In cyber security, a red team is a group of people who play the role of an attacker and provides security feedback from that perspective.

| Type | Description | Timing | Resources | Suitable for |
|---|---|---|---|---|
| **Full-live** | Exercise plan incorporates real scenarios and injects into the exercise. Paper injects only used to stimulate if necessary | Planning: 6–12 months. | Full-live | Exercise plan incorporates real scenarios and injects into the exercise. Paper injects only used to stimulate if necessary |

Typically, organizations will, as they (and/or the technology that they develop) mature, progress from the smaller table-top exercises to the more complicated, full live exercises.

## 2.2 Planning and preparation of exercises

To plan and prepare a cyber event exercise, the following tasks need to be accomplished:

1. Select the exercise scenario(s).
2. Select the exercise type (table-top, full live or hybrid).
3. Define the exercise objectives and intended outcome.
4. Identify the exercise participants (organisations and individuals).
5. Identify logistical needs and required resources.
6. Produce necessary training material.

The exercises will then be executed and evaluated. The documents from MITRE [1] and NIST [2] provide excellent guidance on how to do this.

# 3 Scenarios

In this section, we provide a list of scenarios that can be used when designing cyber event exercises that are relevant for the partners in the CySiMS project. All the scenarios are within the scope of one or more of the project demonstrator cases, as they have been described in [3].

The scope of the scenarios has been restricted to events that will affect one or more of the end users in the project demonstrator cases. This means that potential failure cases that do not require any human interaction, because they will be detected and managed on lower levels, have not been included in the list.

## 3.1 Intended exercise participants

The following end users are envisioned to take part in the exercises:

- PKI Ops, who will operate the PKI service (Case 0)
- PKI-unit supplier, who will manufacture and deliver the PKI-units (Case 0)
- Service engineer, which is the user who will install and configure the PKI-unit on the ships (Case 0).
- Ship crew, who needs to manage situations that occur during the lifetime of the PKI-unit (Case 0).
- Ship crew, who will monitor and interpret messages from other ships (Case 1).
- VTS user, who will monitor and interpret messages from ships and other shore users (Case 1).
- MSW user, who will receive and process the ship reports (Case 2).

As will be seen in the next subsection, not all users are expected to participate in all exercises.

## 3.2 Scenarios for Demonstrator Case 0 (PKI and certificate management)

This business case is designed to demonstrate the main functionality of the PKI and certificate management. The main case that will be demonstrated is *how to enrol a ship into the PKI*. This process is expected to be performed by a service engineer on the ship, who uses specialised software on a laptop to interact with the PKI-unit to submit a CSR, which will be reviewed and signed by the PKI Ops. The signed certificate will then be fetched and installed in the PKI unit by the service engineer. In addition to this main case, we

have also included an additional failure scenario where the PKI unit breaks down after it has been installed on the ship.

Table 2 includes the most relevant scenarios describing what can go wrong, whom of the end users that needs to be involved to solve the problem and which type of exercises we recommend for these scenarios.

**Table 2 Scenarios for Demonstrator Case 0 (PKI and certificate management)**

| Id | Scenario(s) | End user(s) involved | Recommended exercise | Comment |
|---|---|---|---|---|
| **0.1** | Certificate server unavailable:<br>• Vessels cannot fetch and install signed certificates.<br>• Vessels cannot download and update certificate caches.<br>• Newly signed certificates cannot be made available. | Service engineer, PKI Ops | Table-top | How to handle this scenario should be discussed internally by the individual organisations. |
| **0.2** | CSR server unavailable:<br>• Vessels cannot request new certificates.<br>• Pending CSRs cannot be signed. | Service engineer, PKI Ops | Table-top | How to handle this scenario should be discussed internally by the individual organisations. |
| **0.3** | Failing to verify a submitted CSR:<br>• The CSR has an invalid format.<br>• The CSR is from an unsupported flag state.<br>• Incorrect combination of public key and PKI unit ID<br>Wrong or expired activation code. | PKI Ops | Full-live. | These scenarios are easy to test with the PKI server prototype. |
| **0.4** | Loss of trust in the Root CA<br>• Private key has been compromised.<br>• Loss of (or unable to access) private key.<br>• Weaknesses in the cryptographic algorithms. | PKI Ops, PKI-unit supplier, Service Engineer | Table-top | How to handle this scenario should be discussed and agreed upon by all the involved organisations. |
| **0.5** | Loss of trust in an Intermediate CA<br>• Private key has been compromised.<br>• Loss of (or unable to access) private key.<br>• The actor operating the CA is misbehaving. | PKI Ops | Table-top | How to handle this scenario should be discussed internally in the organisation. |
| **0.6** | Accidental revocation of certificates:<br>• Accidently revocation of an Intermediate CA certificate.<br>• Accidently revocation of an end entity certificate. | PKI Ops | Hybrid | How to handle this scenario should be discussed agreed upon by the organisation. The scenario can also be tested (using a dedicated test CA). |

| Id | Scenario(s) | End user(s) involved | Recommended exercise | Comment |
|---|---|---|---|---|
| **0.7** | PKI-unit unavailable or malfunctioning (during installation or service)<br>• CSR cannot be generated.<br>• Signed certificates cannot be installed.<br>• Certificate cache cannot be updated. | Service engineer, PKI-unit supplier | Table-top | How to handle this scenario should be discussed internally in the organisation. |
| **0.8** | PKI-unit unavailable or malfunctioning (after being installed on ship)<br>• Signatures on received messages cannot be verified.<br>• Transmitted messages cannot be signed.<br>• Encrypted channels cannot be established. | Ship crew, PKI-unit supplier | Table-top | How to handle this scenario should be discussed and agreed upon by both the involved organisations. |

## 3.3 Scenarios for Demonstrator Case 1 (intended route) and Case 2 (ship reporting)

The first demonstrator case (intended route) is designed to demonstrate how a ship (autonomous or conventional) broadcasts its intended route, e.g., every 40 seconds or as soon as some data changes. The receivers of these broadcast messages will be other ships and the VTS in the nearby area. In the CySiMS SE project, we will demonstrate how such messages will be signed before being transmitted, and that the signatures can be verified by the receivers.

The second demonstrator case (ship reporting) is designed to demonstrate mandatory ship reporting to the Maritime Single Window (MSW). It is the Nav-station of the ship that will generate the report, utilizing its PKI unit to generate a cryptographic signature, which it will append to the message before it is transmitted to the MSW. Similarly, the MSW will utilize its own PKI-unit to sign an acknowledgement, which will be returned to the ship.

Table 3 includes the most relevant scenarios describing what can go wrong in these two business use cases, whom of the end users that needs to be involved to solve the problem and which type of exercises we recommend.

**Table 3 Scenarios for Demonstrator Case 1 (intended route) and Case 2 (ship reporting)**

| Id | Scenario(s) | End user(s) involved | Recommended exercise | Comment |
|---|---|---|---|---|
| **1.1** | Ship receives a broadcasted "intended route" message without a signature. | Ship crew | Table-top | This will probably be a normal situation. |

| Id | Scenario(s) | End user(s) involved | Recommended exercise | Comment |
|---|---|---|---|---|
| **1.2** | Ship receives a broadcasted "intended route" message with a signature that cannot be verified[2]. | Ship crew | Hybrid | How to handle this scenario should be discussed internally in the organisation. The scenario is also easy to test IRL. |
| **1.3** | VTS receives a broadcasted "intended route" message without a signature. | VTS user | Table-top | This will probably be a normal situation. |
| **1.4** | VTS receives a broadcasted "intended route" message with a signature that cannot be verified[2]. | VTS user | Hybrid | How to handle this scenario should be discussed internally in the organisation. The scenario is also easy to test IRL. |
| **1.5** | MSW receives a "ship report" without a signature | MSW user | Table-top | This will probably be a normal situation. |
| **1.6** | MSW receives a "ship report" with a signature that cannot be verified[2]. | MSW user | Hybrid | How to handle this scenario should be discussed internally in the organisation. The scenario is also easy to test IRL. |
| **1.7** | PKI-unit unavailable or malfunctioning on the ship.<br>• Signatures on received messages cannot be verified.<br>• Transmitted messages cannot be signed.<br>• Encrypted channels cannot be established. | Ship crew | Table-top | *See scenario 0.8.* |
| **1.8** | PKI unit unavailable or malfunctioning at the VTS.<br>• Signatures on received messages cannot be verified.<br>• Transmitted messages cannot be signed.<br>• Encrypted channels cannot be established. | VTS user | Table-top | How to handle this scenario should be discussed internally in the organisation |

[2] There may be many reasons why a signature cannot be verified, including (but not limited to) 1) the corresponding public key certificate is missing from the PKI unit certificate cache, or, 2) the signature has been generated with an expired public key certificate, or, 3) the signature has been generated with a certificate that have been revoked. However, the end user is unlikely to understand, or does not even need to know, the underlying reason for this event; rather he would be presented with a common error message on the screen, such as "INVALID SIGNATURE". We have therefore chosen to merge all these potential failure cases into one single scenario.

| Id | Scenario(s) | End user(s) involved | Recommended exercise | Comment |
|---|---|---|---|---|
| **1.9** | PKI unit unavailable or malfunctioning at the MSW.<br>• Signatures on received messages cannot be verified.<br>• Transmitted messages cannot be signed.<br>• Encrypted channels cannot be established. | MSW user | Table-top | How to handle this scenario should be discussed internally in the organisation |

# 4 Selected exercises for demonstration

Two of the above scenarios have been selected for further detailing in this report. These may (or may not) be executed during the project demonstrations, depending on the interest and availability of the project partners.

## 4.1 Example 1 (table-top): Root CA private key problems

In this example, we show how the scenario "Loss of trust in the Root CA " (scenario 0.4) can be developed into an exercise. Due to the severity and complexity of such a scenario, we have proposed that is performed as a table-top exercise.

**Exercise objectives and intended outcome**: The main objective of this exercise is to prepare for a situation where the integrity of the Root CA has been compromised. Such a situation could occur, for example if the Root CA private key has been leaked, or if it has been discovered that the selected cryptographic algorithms have severe weaknesses that will reduce the trust in the system. The intended outcome of the exercise is to prepare and plan for such events, to be able to continue the operation of the PKI and to restore the affected stakeholders' trust in the system.

**Exercise participants**:

- PKI Ops: one or more persons who are working with the day-to-day operations of the PKI services.
- PKI supplier: one of more persons who are responsible for the manufacturing and delivery of the PKI units.
- Service engineer: one of more persons who are responsible for installing and/or re-configuring the PKI units on the ships.

**Logistical needs and required resources**:

- A conference room and audio/visual equipment.

**Necessary training material**:

- Briefing material, including an agenda for the exercise and an introduction to the CySiMS PKI.
- Facilitator guide, including the objectives and intended outcome of the exercise, the exercise scenario and a list of questions regarding the scenario, which address the exercise objectives. For this exercise, relevant questions are:
    - *What could be the reason for such a situation?*
    - *How would such a situation be detected?*
    - *Who will need to be notified (who are the key points of contact)?*
    - *Who will be responsible for what (delineate roles and responsibilities)?*
    - *How do we communicate (with customers, vendors, executives, the public media, etc)?*
    - *How do we do certificate replacement?*

    - *How do we migrate to a new Root CA?*
- Participant guide, including the same information as the facilitator guide, but without the list of questions.
- Evaluation report, which will be populated by the facilitator after the exercise.

Note that documents describing "best practice" for preparing and responding to a Root CA compromise scenario already exist (see for example [4]) but would need to be adapted to the maritime context.

## 4.2 Example 2 (hybrid): Intended route - invalid signatures

In this example, we show how the scenario " Ship receives a broadcasted "intended route" message with a signature that cannot be verified" (scenario 1.2) can be developed into an exercise. Due to the relatively simplicity of simulating such a scenario, we have proposed that is performed as a hybrid exercise, which in this case will be a table-top exercises, but with the inclusions of live events.

**Exercise objectives and intended outcome**: The main objective of this exercise is to train the ship crew to handle situations where the PKI-unit on the ship cannot verify the signature of one or more received "intended route" messages. As explained in footnote **Error! Bookmark not defined.**, there are several reasons why such a situation could occur. The intended outcome of the exercise is to prepare and plan for such events, so that the ship crew are familiar with the situation and know how to react.

**Exercise participants**:

- Ship crew
- "Red team" (preparing and transmitting the invalid "intended route" messages during the live part of the exercise)

**Logistical needs and required resources**:

- A conference room and audio/visual equipment.
- Two Single Board Computers (SBC) for transmitting and receiving "intended route" messages (in S-421 format). The transmitting computer must be capable of adding invalid signatures to the messages. Both computers need to be able to communicate directly with each other (hence avoiding the need for VDES radios)
- Network connectivity (for the SBCs).

The exercises can take place in the conference room, where the SBCs will be used for the live events.

**Necessary training material**:

- Briefing material, including an agenda for the exercise and an introduction to the use of the S-421 message format for "intended route" messages.
- Facilitator guide, including the objectives and intended outcome of the exercise, the exercise scenario and a list of questions regarding the scenario, which address the exercise objectives. For this exercise, relevant questions are:
    - *Where is the signature field on the "intended route" messages?*
    - *What does it mean that a message has been signed?*
    - *What does it mean when the signature is valid/invalid/missing?*

  During the live exercise, when an invalid signature is received:
    - *What is happening here?*
    - *What do you do now?*
    - *How can you verify whether the message is correct?*
- Participant guide, including the same information as the facilitator guide, but without the list of questions.
- Evaluation report, which will be populated by the facilitator after the exercise.

Note that there does not yet exist any specification of how the SBCs are to indicate the status of the signatures on the messages that they receive. Here, we have assumed that the computers will have the ability to display errors to the users.

## 5 References


[1] Cyber Exercise Playbook. The MITRE Corporation. November 2014. Available at https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

[2] NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. Recommendations of the National Institute of Standards and Technology. September 2006

[3] CySiMS SE project deliverable. D1.1 Plan for the operational pilot. Version 0.4, 2020-12-20.

[4] Paul Turner, et.al. Preparing for and Responding to CA Compromise and Fraudulent Certificate Issuance. NIST Pubs, ITL Bulletin, July 10, 2012. Available at https://www.nist.gov/publications/preparing-and-responding-ca-compromise-and-fraudulent-certificate-issuance