*Document No:*

*Title: Cybersecurity in STM*

*Date: 2018-02-20*



Table of Contents

1 What is cybersecurity? 3

2 Security domains in STM 4

2.1 SeaSWIM security domain 4

2.2 Ships security domain 4

2.3 Service providers security domain 4

3 Cybersecurity in SeaSWIM domain 5

3.1 Encryption 6

3.2 Certificates in SeaSWIM 7

4 STM principal use case 8

# What is cybersecurity?

Several definitions can be found on the internet, below are a few examples.

Preservation of confidentiality, integrity and availability of information in the Cyberspace. *(ISO/IEC)*

Cybersecurity refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. *(webopedia)*

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. *(Merriam-Webster)*

The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. *(US - NICE)*

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability

- Integrity, which may include authenticity and non-repudiation

- Confidentiality

*(ITU)*

Four objectives:

- Tackling cybercrime and making (the UK’s) cyberspace secure for business;

- Becoming more resilient to cyber attacks and “better able to protect [the UK’s] interests in cyberspace”;

- Creating an “open, stable and vibrant cyberspace which the [UK] public can use safely and that supports open societies”; and

- Having “the cross-cutting knowledge, skills and capability” to underpin the other three objectives

*(Adapted from the UK 2011 Cybersecurity Strategy)*

# Security domains in STM



## SeaSWIM security domain

SeaSWIM – Sea System Wide Information Management is the regulated security domain in STM which all actors are obliged to comply with in order to be SeaSWIM compliant. SeaSWIM is built upon the Maritime Connectivity Platform (MCP) which provides functions for identification and supports authentication.

## Ships security domain

Basically this is up to the Ship/bridge system provider, e.g. ECDIS provider, facilitating the communication with ships onboard systems. Although using the standardized information services developed within STM, like VIS (Voyage Information Service) and SPIS (Ship Port Information Service), security functions are developed and possible to utilize for securing communication to ships.

## Service providers security domain

Possibilities exist as described above, although the transfer of information (routes, text messages etc.) is probably done in the context of an existing agreement with a service provider stating the level of security required.

# Cybersecurity in SeaSWIM domain

*Cybersecurity in SeaSWIM addresses confidentiality & integrity (by encrypting the communication), authentication (of registered identities) and authorization.*

* **Confidentiality** ensures that no one else than the intended recipient can read and understand the content of the document. Confidentiality corresponds to the sealed envelope.
* **Integrity** ensures that the content of the document has not been changed since it was issued. Integrity corresponds to the difficulties in changing printed text on paper.
* **Authentication** is any process by which a system verifies the identity of a user (human or machine) who wishes to access it (i.e. to confirm, You are who You claim to be, like a passport). This corresponds to the written signature and official stamp on paper.
* **Identification** refers to the act of stating a person or thing’s identity.
* **Authorization** is the process of determining a set of permissions that is granted to a specific trusted identity.

Confidentiality is facilitated in SeaSWIM by use of an encrypted communication between authenticated parties in MCP by use of host certificates.

Integrity measures are not implemented in SeaSWIM, since this would add a level of complexity and incur delays in the STM validation project implementation (integrity means actually encrypting the message content in addition to encryption the communication).

Authentication is based on instance certificates issued to each exposed service provider’s service instance registered in MCP (i.e. Ship, VTS).

Identification is realized by registering an organization and related users in MCP.

Authorization to information is handled by each service provider (onboard/ onshore operator), the owner of the information grants authenticated actors access to each information object (i.e. a route, dirway etc.). The adjacent information service (VIS, SPIS etc.) facilitates this, providing an Access Control List table in storing which stakeholder have access to specified information.

## Encryption

In STM the communication is encrypted using host-certificates issued in the Maritime Connectivity Platform (MCP) by each identified stakeholder hosting services (shipping company, ECDIS manufacturer, VTS, service provider etc.).

These host certificates are used to create an encrypted link between a service consumer and service provider based on SSL (Secure Sockets Layer). SSL certificates have a unique key pair\*: a public and a private key. These keys work together to establish an encrypted connection. The larger the size of the keys the more secure the connection is.

Furthermore encryption can be made using asymmetric or symmetric keys.

* Asymmetric encryption (or public-key cryptography) uses a separate key for encryption and decryption. Anyone can use the encryption key (public key) to encrypt a message. However, decryption keys (private keys) are secret. This way only the intended receiver can decrypt the message.
* Symmetric encryption (or pre-shared key encryption) uses a single key to both encrypt and decrypt data. Both the sender and the receiver need the same key to communicate.

In SeaSWIM the SSL encryption used results in a sequence as shown below in encrypting the link between each service, using asymmetric encryption for the handshake and then symmetric encryption for the established session. In the picture the Web browser corresponds to the requesting service, the link is encrypted by use of host certificates.



*(Digicert)*

1. Server sends a copy of its asymmetric public key to browser
2. Browser creates a symmetric session key and encrypts it with the server’s asymmetric public key then sends it to the server.
3. Server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.
4. Server and browser now encrypt and decrypt all transmitted data with the symmetric session key. This allows for a secure channel because only the browser and the server know the symmetric session key, and the session key is only used for that specific session. If the browser was to connect to the same server the next day, a new session key would be created.

*\* Cryptographic algorithms depend on the fact that prime factorization of large numbers takes a long time. Basically you have a "public key" consisting of a product of two large primes used to encrypt a message, and a "secret key" consisting of those two primes used to decrypt the message. You can make the public key public, and everyone can use it to encrypt messages to you, but only you know the prime factors and can decrypt the messages. Everyone else would have to factor the number, which takes too long to be practical, given the current state of the art of number theory.*

## Certificates in SeaSWIM

STM certificates are created using MCP, these can be issued for devices, vessels, users, organizations and services. The certificates can be used as either host certificates or instance certificates, host certificates handles the encryption/ decryption (as described above) and instance certificates facilitates the authentication of the calling organization.

A host is typically a server hosting a number of service instances i.e. a service provider might install a number of service instances each representing a single ship or perhaps representing two different services like route optimization and route check. The host or server has a host certificate installed to handle encryption/ decryption of the communication whilst each instance has an instance certificate used for authentication when a message is sent from that particular instance. See picture below.



The encrypted communication corresponds to the sealed envelope (encrypted using the sending server host certificate), the envelope contains an unencrypted message (route, textMessage etc.) and the Ship 1 instance certificate. At the receiving end the envelope is opened (decrypted using the symmetric session key) and the Ship 1 instance certificate is verified against the MCP. Additionally the Ship 1 instance certificate is checked against the MCP revocation list to ensure it isn’t revoked. This is due to every certificate has a validity date and/ or can be revoked.

To issue a new certificate for, for example a ship, the administrator of the organization who owns the ship will need to log in to the MCP and use its functionality for issuing new certificates. The same goes for revoking a certificate.

Furthermore the server is protected by a firewall restricting communication only to accept encrypted communication (SSL).

Realizing authentication by use of instance certificates as above creates a so called Public Key Infrastructure PKI, there are ways of ensuring authentication without the use of certificates though. One of the most popular is simply using a user and password. However this is a rather weak protection since passwords and usernames are easier compromised and thus not so well suited for machine to machine communication.

# STM principal use case

Below picture briefly explains how a ship utilizes a route optimization service in SeaSWIM using certificates.



1. Find the route optimization service by issuing a lookup to the MCP service registry.
2. An encrypted communication is established with the MCP service registry (using the host certificate at the sending side - SSC)
3. The findservice query is sent inside the encrypted communication (sealed envelope)
4. In MCP the communication is decrypted using the host certificate residing in the in MCP identity registry
5. The findService result is returned over the established encrypted communication
6. Send route to the route optimization service provider (callService)
7. An encrypted communication is established with the service provider (using the host certificate)
8. The route message is sent together with the sending party service instance certificate (ships instance certificate)
9. At the service provider end the communication is decrypted (using the receiving side host certificate) and the instance certificate is verified against authenticated users in MCP identity registry including checking the certificate revocation status
10. The route is then optimized according to service providers parameters
11. Receive optimized route
12. The route optimization service application grants access to the optimized route for the calling ship (in case the route is to be optimized continuously)
13. An encrypted communication is established with the ship (using the host certificate at the service provider side)
14. The optimized route message is sent together with the sending party service instance certificate (service provider instance certificate)
15. In the SSC for the ship, the communication is decrypted (using the host certificate installed) and the service provider certificate is verified against authenticated users in MCP identity registry together with the revocation status check.
16. The optimized route is forwarded to the ship for evaluation