

# **STCW EU Seafarers' Certification Platform**

## **High Level Functional Description**

V 0.8

**Date: 27 May 2022**

## Table of Contents

<b>Definitions</b>	4
Certificate	4
CoC - Certificate of competency	4
CoP - Certificate of proficiency	4
Dispensation	4
Eal - Endorsement attesting the issue	4
EaR - Endorsement attesting the Recognition	4
Electronic seal (eSeal)	4
Electronic signature (eSignature)	4
(Maritime) Administration	4
Member States Local Systems	4
MET - Maritime Education and Training institutions	4
Original form of any certificate required by the Convention	5
Printed version of electronic certificate	5
PSCO - Port State Control Officer	5
QESeal - Qualified Electronic Seal	5
QESign - Qualified Electronic Signature	5
Seafarer	5
Seafarer Electronic certificate	5
Unique tracking number	5
Validation	5
Verification	5
<b>Concept</b>	6
Actors	6
Context Diagram	7
Central Node	7
Central Hub	8
Adoption options	8
Dataset	9
Generic Requirements	9
<b>Central Node</b>	10
Provide functions aiming the central management and storage of certificates	10
Types of Certificates that shall be supported	10
Certificates' Management and Storage Functions	10
Document upload, storage, validation and approval workflows	11
Provide functions aiming the eSignature and/or eSeal of certificates	11
Electronic Signature of Certificates (eSignature and/or eSeal)	11
Provide multi-tenant capacities	12
Provide functions allowing data integration into the STCW-IS	12

<b>Central Hub</b> .....	12
Provide functions allowing certificates' search and verification at EU level (Central Node + Member States Local Systems) .....	12
Certificates' Search and Verification across EU Level.....	12
Provide functions for transparent integration with Member States Local Systems.....	13
Provide functions allowing for an online application for a certificate .....	13
Provide functions allowing integration with THETIS .....	13
<b>High level Processes</b> .....	14
Apply for a certificate.....	14
Create a certificate .....	14
Electronically Sign and/or Seal a Certificate .....	14
Verify eCertificate authenticity and validity .....	15
<b>ANNEX I User profiles</b> .....	17
<b>ANNEX II Dataset</b> .....	18

## Definitions

### Certificate

Means a valid document, by whatever name it may be known, issued by or under the authority of the Administration or recognized by the Administration authorising the holder to serve as stated in this document or as authorised by national regulations.

### CoC - Certificate of competency

A certificate issued and endorsed (attesting the issue) to masters, officers and GMDSS radio operators in accordance with the provisions of chapters II, III, IV or VII of the Annex to the STCW Convention and entitling the lawful holder thereof to serve in the capacity and perform the functions involved at the level of responsibility specified therein.

### CoP - Certificate of proficiency

A certificate, other than a certificate of competency issued to a seafarer in accordance with chapters II, III, V, VI or VII of the Annex to the STCW Convention, stating that the relevant requirements of training, competences or seagoing service in the Convention have been met.

### Dispensation

A document permitting a seafarer to serve in a capacity for which he/she does not hold the appropriate certificate.

### Eal - Endorsement attesting the issue

An endorsement required by Article VI of the STCW Convention to attest the issue of a certificate for masters and officers.

### EaR - Endorsement attesting the Recognition

An endorsement of a certificate of competency or of a certificate of proficiency issued to masters and officers in accordance with the provisions of regulations V/1-1 and V/1-2 of the Annex to the STCW Convention.

### Electronic seal (eSeal)

Means data in electronic form which is attached to, embedded in, or logically associated with, other electronic data to serve as a method of guaranteeing the origin and the integrity of the electronic data. Electronic seals can be simple, advanced or qualified.

### Electronic signature (eSignature)

Means data in electronic form which is attached to, embedded in, or logically associated with, other electronic data to serve as a method of authentication of the issuer and contents of the electronic data. Electronic signatures can be simple, advanced or qualified.

### (Maritime) Administration

Means the Government of the State whose flag the ship is entitled to fly.

### Member States Local Systems

Means the system(s) in which the certificates issued to seafarers in each Member States are registered and managed.

### MET - Maritime Education and Training institutions

Institutions providing education and training to seafarers.

#### Original form of any certificate required by the Convention

Means a certificate issued in paper or electronic form in the format approved by the Administration, provided that the minimum information, as required in paragraph 4 of section A-I/2 of the STCW Code, is readily available.

#### Printed version of electronic certificate

Means a printout produced from the electronic certificate.

#### PSCO - Port State Control Officer

Is a properly qualified person, authorised to carry out port state control inspections.

#### QESeal - Qualified Electronic Seal

Means a type of electronic seal (eSeal) that serves as evidence that an electronic document was issued by a legal entity ensuring certainty of the document's origin and integrity. It is based on a qualified electronic certificate and created by a Qualified Electronic Signature Creation Device (QSCD). It is provided only by an accredited Qualified Trust Service Provider. The main difference with a Qualified Electronic Signature is that the eSeal binds to a legal entity and the eSignature to an individual (a natural person).

#### QESign - Qualified Electronic Signature

Means a type of electronic signature (eSignature) that, by EU regulation, has the same legal effect than the handwritten signature. A QES is an Advanced Electronic Signature based on a qualified electronic certificate and created by a Qualified Electronic Signature Creation Device (QSCD). It is provided only by an accredited Qualified Trust Service Provider.

#### Seafarer

Any person who is employed or engaged or works in any capacity on board a ship.

#### Seafarer Electronic certificate

Means a certificate issued in an electronic format established/approved/ by the Administration to ensure viewing compatibility for all intended viewers.

#### Unique tracking number

Means a string of numbers, letters or symbols used as an identifier to distinguish an electronic certificate issued by or under the authority of an Administration from any other electronic certificate issued by or under the authority of the same Administration.

#### Validation

Means the analysis of the data gathered, including of any necessary documentary evidence, to ensure that the certificates are issued only to candidates who comply with the requirements. The validation will result in the definition of the applicable limitations and of the certificate validity period.

#### Verification

Means a reliable, secure and continuously available process to confirm the authenticity and validity of an electronic certificate using the unique tracking number and other data contained on or embedded in the electronic certificate.

## Concept

The objective of the project is to set up and host an **EU Seafarers' Certification Platform** to facilitate the issue of certificates to seafarers in a digital format. The development of such a platform will offer a complement or alternative to the redesigning or enhancement of national register systems by the individual Member States with all the involved costs while promoting the establishment of eCertification at EU level.

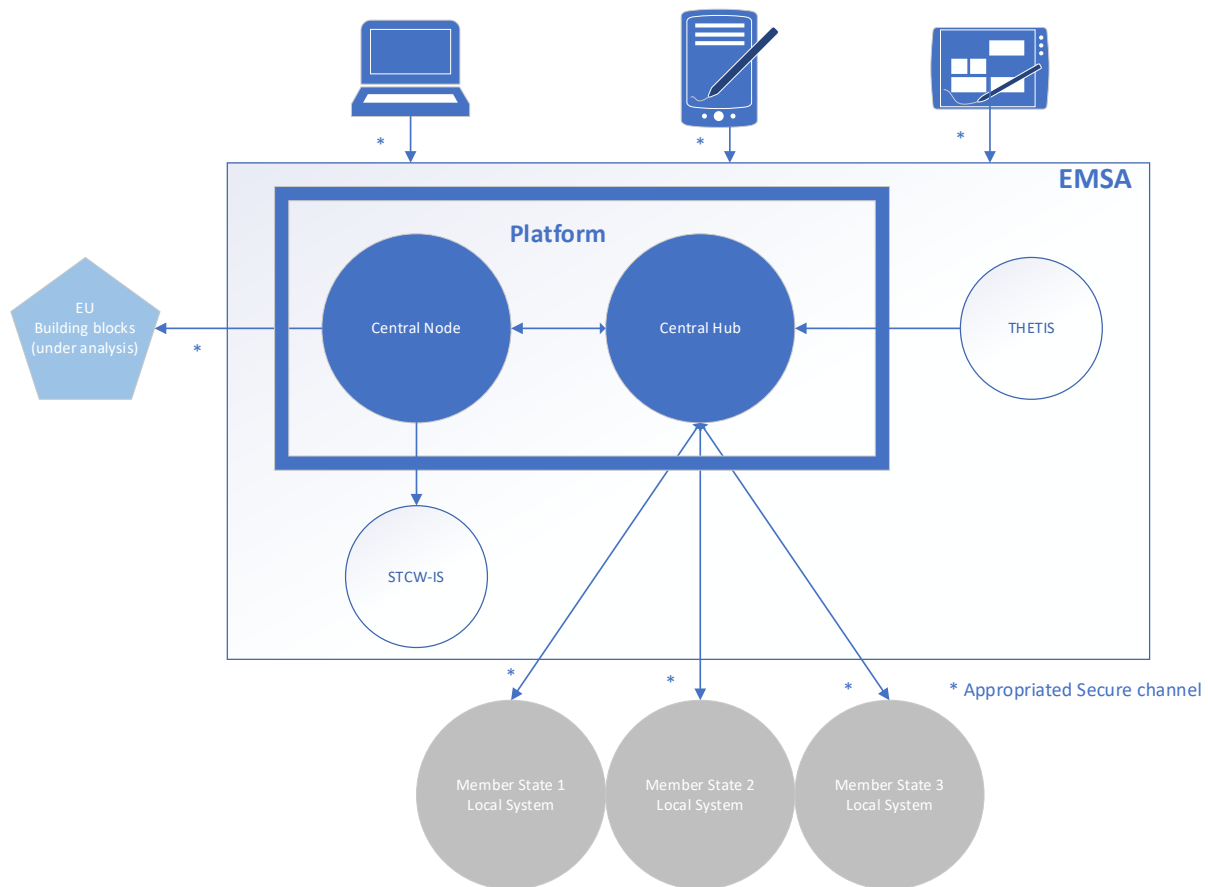
The modular development of the platform will allow Member States to choose which functions they would like to use (please refer to the “**Adoption options**” section below).

## Actors

- Seafarers
- EU maritime administrations
- Non-EU maritime administrations
- Companies
- Medical practitioners
- Maritime education and training institutions
- Port State Control Officers
- Other enforcement authorities

Each actor will have different profiles/roles (see **ANNEX I User profiles** for further details).

## Context Diagram



## Central Node

The EU Seafarers' Certification Platform Central Node (Registry) shall implement functionalities to:

- Provide functions aiming the central management and storage of any certificate issued by or under the authority of an Administration
- Provide functions aiming the central management and storage of the documentation related with the certificate issuing lifecycle
- Provide functions aiming the eSignature and/or eSeal of the certificates issued to seafarers through a "Qualified Electronic Signature" and/or "Qualified Electronic Seal" using a workflow
- Provide multi-tenant capacities (each Member State shall have its dedicated and isolated area)
- Provide the ability to configure certificates' attributes, parameters and layouts per Member State
- Provide the ability for seafarers to authorise the sharing of their data with different actors
- Provide the ability for the requirements for certification as per the Member States' national legislation (for workflows or the content of code lists), to be configurable by each country
- Provide functions aiming the cross fertilisation of information by other stakeholders intervening in the issuing of the certificates such as companies, medical practitioners or Maritime Education and Training institutions
- Provide functions allowing data integration into the STCW-IS

Please refer to the “**Central Node**” section below for further details on these functionalities

## Central Hub

**EU Seafarers' Certification Platform** Central Hub shall implement functionalities to:

- Provide certificate search functions across the EU
- Provide functions allowing for an online verification at EU level (via a connection to the Platform Central Node or to the Member States Local Systems)
- Allow transparent integration with the Member States Local Systems
- Provide functions allowing for an online application for a certificate to be made from seafarers and/or companies
- Provide functions allowing integration with THETIS

Please refer to the “**Central Hub**” section below for further details on these functionalities

## Adoption options

Member States can choose how they plan to use the **EU Seafarers' Certification Platform**. Relevant options include:

- **Member State decides to fully adopt the EMSA Seafarers' Certification Platform:**
  - It will allow online application for the certificate from seafarers and/or companies
  - It will create new digital certificates using the EMSA Central Node facility
  - It will store all issued certificates in EMSA within its dedicated and isolated area
  - It will store all documents supporting the issue of the certificates
  - It will sign and/or seal the new certificates using the EMSA Central Node facility

A migration process of the existent certificates might be setup

- **Member State decides not to use the EMSA Central Node for the creation and registry of certificates but only to eSign/eSeal certificates and to be connected to EMSA's Search and Verification facility**
  - It will transfer and store only the data contained in the certificates to be digitalised to a dedicated and isolated storage area in the Central Node facility
  - It will sign and/or seal the new certificates using the EMSA Central Node facility
  - Interfaces will be established between EMSA and the Member States Local Systems for the eCertification, Search and Verification functions



- **Member State decides not to use the EMSA platform but would only like to be connected to the EMSA's Search and Verification facility**
  - An interface will be established between the EMSA and the Member States Local Systems for Search and Verification functions

## Dataset

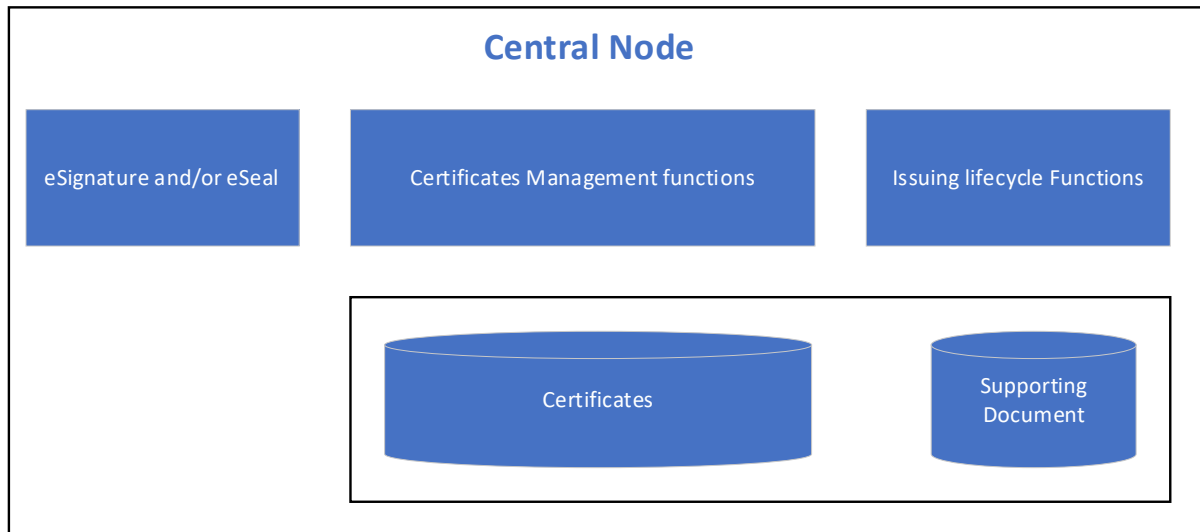
As a first step the **EU Seafarers' Certification Platform** will include the certificates issued by the Member States under the STCW Convention. The dataset included as in **ANNEX II Dataset** to this document lists the generic elements defined in the Convention, that will need to be further detailed by the Member States.

## Generic Requirements

The **EU Seafarers' Certification Platform** shall support:

- The use of multiple languages (EU official languages with English being the common language used). National language support shall be used for all functions such as sorting, searching and comparing
- The integration with other EMSA systems for usage of standard reference data
- The interoperability with external systems
- User authentication using an electronic identity service or an internal login (with the password being sent to the registered e-mail)
- Communications/notifications to be sent to users (as part of a workflow), should the user adhere to it
- Configuring different workflows per functionality and per process of the platform
- Extracting reports for information purposes such as number of certificates issued, contact details of approved maritime training and education institutions, etc
- Being displayed and used in tablets and mobile phones
- The display of different dashboards depending on the user profiles/roles
- Compliance with the rules on personal data protection by establishing a system-wide authorisation solution
- Compliance with the EU Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data
- The processing of personal data that requires special measures of protection
- The use of security standards for system and application access control, such as https, OAuth 2.0 and openId Connect
- Compliance with ISO/IEC standards as much as possible (to be detailed during the project specifications)
- The standardisation (as much as possible) of lists and options
- Features for gathering Historical and Audit information
- Features to prevent fraud and enough security measures that allow for some sort of resistance to cyberattacks
- System shall be available 24x7 with an yearly availability of 99.9%

## Central Node



## Provide functions aiming the central management and storage of certificates

### Types of Certificates that shall be supported

The scope of the EU Seafarers' Certification Platform includes all certificates issued by the EU maritime administrations.

### Certificates' Management and Storage Functions

As per the decision taken by the participating countries (see **Adoption options** above), the management and storage functions will cover two types of storage:

- complete administrative processes and full certificate and document storage, including of the documentation related with the certificate issuing lifecycle, for Member States wishing to host their national registry systems at EMSA, and
- storage regarding the data on the certificates that will be issued and duly signed and/or sealed only, for Member States wishing to sign and/or seal their certificates using the EMSA Certification facility.<sup>1</sup>

The Central Node will be the owner of the certificates' data storage.

- **The EU Seafarers' Certification Platform** shall provide the following functionalities
  - Certificates' lifecycle:
    - List and visualisation of requested certificates
    - Checking of eligibility requirements for the issuing/renewal of certificates (validation process)
    - Communication/notification with/to the applicant/holder of the certificate, including the exchange of information should discrepancies in the application process or rectifications in the seafarers' file be deemed necessary
    - Approval and creation of new certificates

<sup>1</sup> The transfer of all data listed under Annex V of Directive 2008/106/EC will exempt Member States from sending it to EMSA annually

- Edition<sup>2</sup> of existent certificates
- List and visualisation of registered certificates
- Authorisation for sharing of data with different actors (e.g. upon a certificate recognition procedure)
- Deletion / revocation / archiving
- Historical and audit functionalities
- Documents' lifecycle:
  - Upload and storage of the documents supporting the issue of the certificates including seagoing service, medical certificates, education and training and identity documents
  - Edition<sup>3</sup> of existent documents
  - List and visualisation of documents
  - Deletion / revocation / archiving
  - Historical and audit functionalities
- Display of different dashboards depending on the permissions per profile/role

Alongside the certificate management and storage functions, other modules might be included in the platform that are currently available at Member States level such as:

- Assessment of competence modules and
- Maritime education and training (MET) approval and monitoring modules

both related with the obligations of the Member States to comply with Regulation I/6 of the STCW Convention

- Registration and calculation of seagoing service time

### Document upload, storage, validation and approval workflows

- The **EU Seafarers' Certification Platform** shall support the storage of both the documents uploaded through the on-line application module at Central Hub level by seafarers and/or companies applying for the issue of a certificate and the documents uploaded at the Central Node level
- The **EU Seafarers' Certification Platform** shall support validation and approval processes of such an application through pre-defined workflows (to be specified at a later stage)

## Provide functions aiming the eSignature and/or eSeal of certificates

### Electronic Signature of Certificates (eSignature and/or eSeal)

- The **EU Seafarers' Certification Platform** shall provide functionalities for Electronic Signature (eSignature) and Electronic Seal (eSeal) of Certificates using a Qualified Electronic Signature and/or Seal, that is compliant with EU Regulation No 910/2014 (eIDAS Regulation) based on CEF building blocks such as CEF eSignature
- eSignature and/or eSign shall only be possible if all information contained in the certificates to be digitalised is provided to the **EU Seafarers' Certification Platform**
- eSignature shall be possible using the **EU Seafarers' Certification Platform** "Electronic Digital keys" or using the Member State Signing Infrastructure. The latter shall require that the Member State has available the Remote Qualified Electronic Signature functions
- eSeal shall be possible using the **EU Seafarers' Certification Platform**, as above

<sup>2</sup> The modification of a certificate that is already signed/sealed with QES will invalidate the existing QES. QES signed/sealed documents cannot be modified and a new document will need to be created and signed/sealed with QES

<sup>3</sup> See above

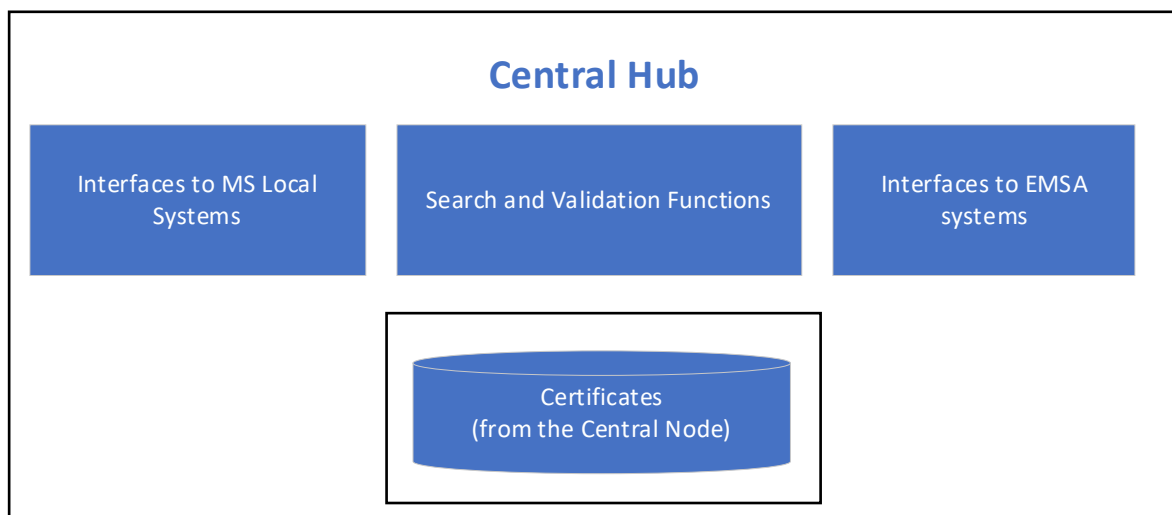
## Provide multi-tenant capacities

- The **EU Seafarers' Certification Platform** shall provide for a dedicated and isolated area per each Member State where it will be able to configure different profiles/roles assigned to the users, workflows, certificates' code lists, attributes, parameters and layouts

## Provide functions allowing data integration into the STCW-IS

- The data on the seafarers' certificates available in the **EU Seafarers' Certification Platform** shall be transparently integrated into the STCW-IS. Moreover:
  - If besides providing certificate detailed data to the **EU Seafarers' Certification Platform** for eCertification purposes, Member States also make available the gender and nationality of the seafarer together with the status of the certificate, there will be no need to provide data to the STCW-IS anymore. Information received shall be anonymized and transparently integrated into the STCW-IS

## Central Hub



## Provide functions allowing certificates' search and verification at EU level (Central Node + Member States Local Systems)

### Certificates' Search and Verification across EU Level

- The **EU Seafarers' Certification Platform** shall provide a seamless certificate search at EU Level by:
  - Searching for certificates in the Platform Central Node (that is the owner of the stored certificates' data)
  - Transparently connect to integrated Member States Local Systems
- The **EU Seafarers' Certification Platform** shall provide functionalities to allow the verification of the authenticity and validity of a "Seafarer Certificate" by:
  - Uploading the certificate document as a file
  - Reading a QR code
  - Entering of an ID<sup>4</sup> and some additional information (e.g. the issuing Member State)

<sup>4</sup> This ID is to be a unique tracking number, as stated in the IMO Guidelines on the use of electronic certificates of seafarers. It should be standardised at EU level and allow an easy identification of the entities issuing the certificate. The unique tracking number and other data for verification should always be available.

- Depending on the data protection restrictions existing in the Members States, the **EU Seafarers' Certification Platform** shall make available two different verification areas:
  - Public area, which is available to all interested parties
  - Private area assessed through username and password.

Depending on the type/permissions of the user, it shall be possible to:

- Only visualise the status of the certificate (e.g., Valid)
  - Get more detailed information
  - Download the certificate file
- The **EU Seafarers' Certification Platform** Search and Verification functionalities shall be available via a multi-channel portal. Two main channels are foreseen:
  - Web Portal
  - Mobile App

## Provide functions for transparent integration with Member States Local Systems

- The **EU Seafarers' Certification Platform** shall transparently integrate Member States Local Systems for:
  - eSignature of certificates with the Member State own Remote Qualified Electronic Signature functions
  - Search and verification of the certificates' authenticity and validity against the Member States Local System
  - Receiving relevant data to feed the **EU Seafarers' Certification Platform**

## Provide functions allowing for an online application for a certificate

- The **EU Seafarers' Certification Platform** shall support an on-line application module for seafarers and/or companies applying for the issue, revalidation, replacement of a certificate or endorsement by:
  - Providing the means for users to request to be registered in the Platform using a registration form
  - Providing the means for users to request to be registered in the Platform using a trustworthy electronic identity authentication
  - Making available a form for users to input the required information
  - Providing for the upload of the supporting documents to be done at Central Node level
  - Providing the means for the 'application process' to run at Central Node level
  - Providing the means for the approval of the application to be done by the competent authority at Central Node level after all the process is completed (including e.g. payment)

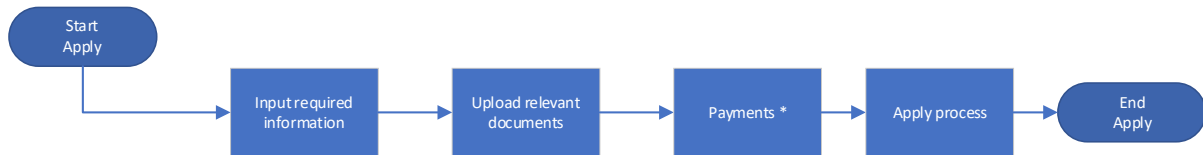
For Member States already making available similar online application portals, the **EU Seafarers' Certification Platform** shall link to the Member States Local System, if possible.

## Provide functions allowing integration with THETIS

- The **EU Seafarers' Certification Platform** shall be transparently integrated with THETIS:
  - THETIS shall be modified to have a transparent integration with the Platform; while conducting an inspection, PSC officers shall be able to verify the certificates' authenticity and validity against the **EU Seafarers' Certification Platform**

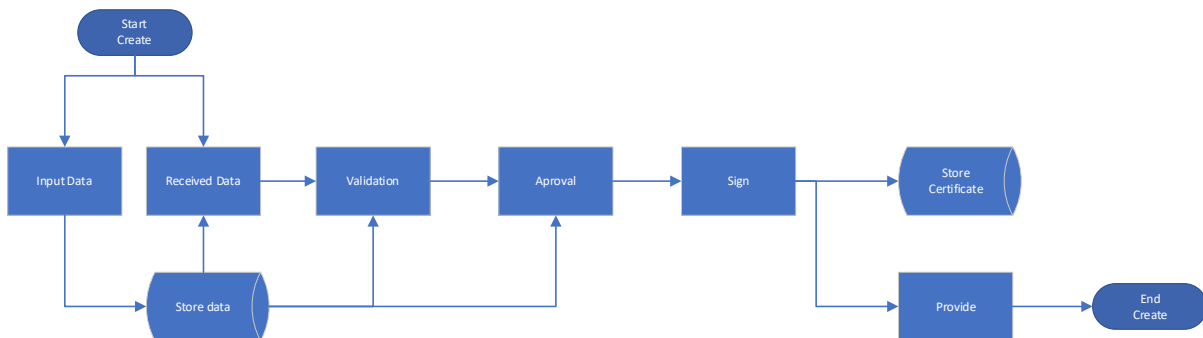
## High level Processes

### Apply for a certificate

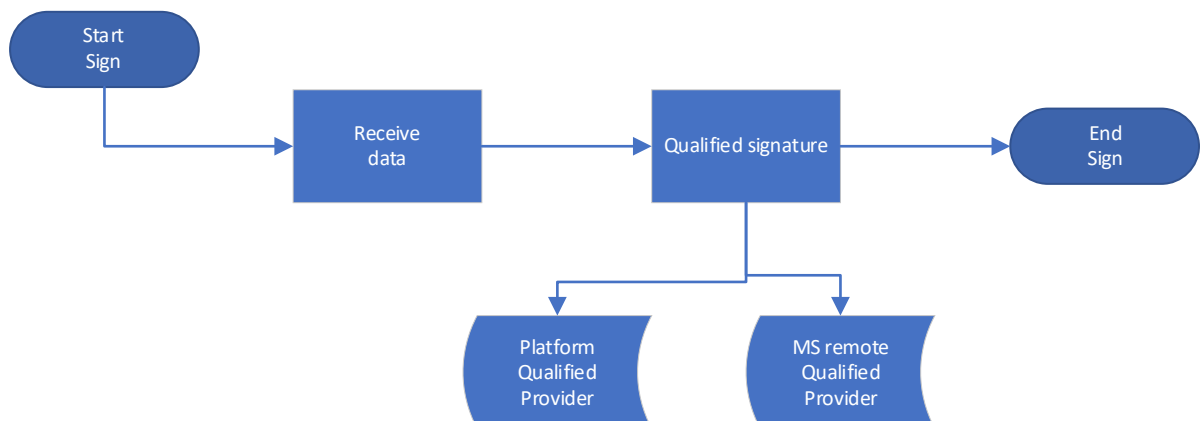


\* to be further discussed with the Member States, as payments are to be managed by each Member State. EMSA's platform might provide information for future processing of the payment but shall not provide billing and payment functionalities

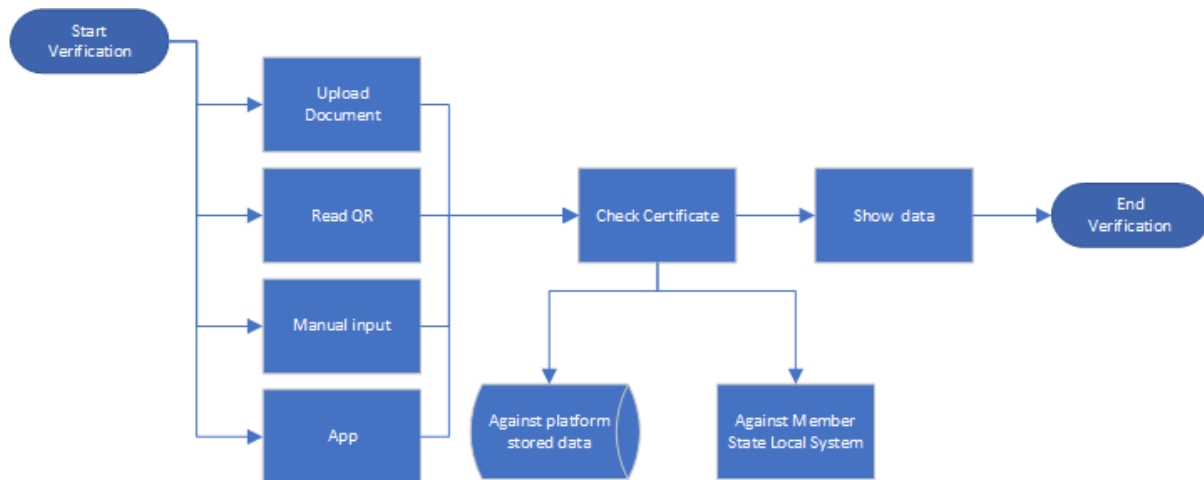
### Create a certificate



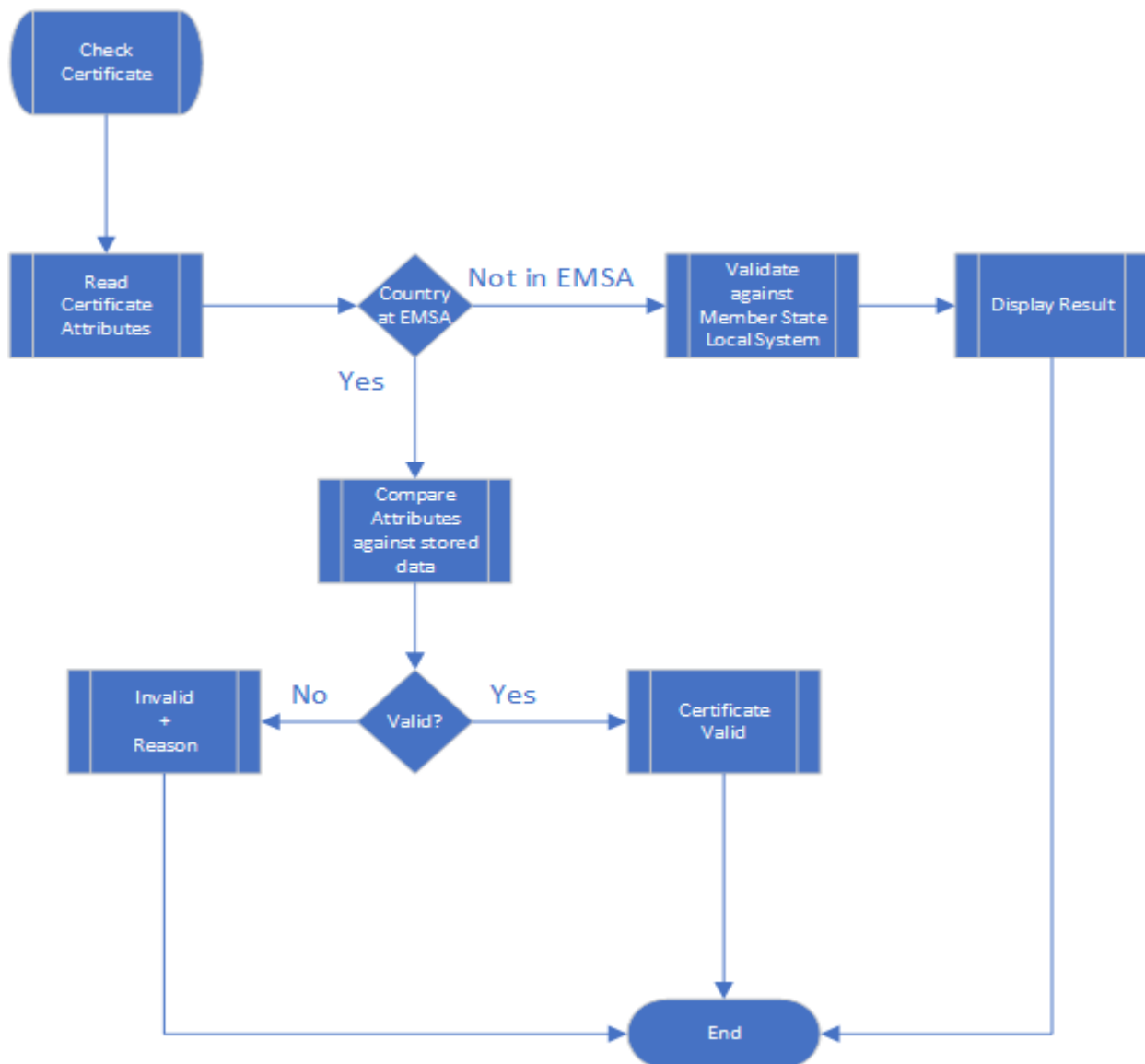
### Electronically Sign and/or Seal a Certificate



## Verify eCertificate authenticity and validity



Regarding the verification process, the dataflow is the following:



Regarding the Certificate Attributes these can be:

- Shared by the following types of certificates: CoC/EaI, EaR, CoP, Dispensations

- Country issuing
- Certificate Number
- Date of issue
- Name of the seafarer
- Date of Expiry (not mandatory in the case of CoPs)

- Or have additional attributes per type of certificate

CoC/EaI, EaR	CoP	Dispensations
Functions (not mandatory and mostly used in the case of certificates issued under Regulation VII of the STCW Convention)	Title or name of the certificate	Name of the vessel
Levels (not mandatory and mostly used in the case of certificates issued under Regulation VII of the STCW Convention)	STCW Regulation or STCW Code section	Capacity
Capacity	Authority issuing the certificate (if different from the authority issuing the other types of certificates)	Limitations
Limitations		

For verification purposes, the rules are the following:

- All the attributes above are mandatory except when stated otherwise. Attributes shall be read from the certificate or be manually entered in the system for validation
- Name of the seafarer must be an exact match (shall take into account the multi-language characteristics of the Platform)
- Capacity and Limitations shall be validated against internal lists that can be different from country to country
- Reading of the QR code, will link directly to the respective validation site
- Function "Compare attributes against platform stored data" will first check the internal status of the certificate. If certificate is not expired, function will compare all attributes read from the certificate with the information stored in the database. If information matches, the certificate will be considered valid.

During the specifications phase, other rules might be defined if so agreed by all MS



## ANNEX I User profiles

The table below details some of the profiles users might have when interacting with the **EU Seafarers' Certification Platform**. Some users might have different profiles. Other profiles might be defined by the Member States

	Seafarers	EU maritime administrations	Companies	Medical practitioners	Maritime education and training institutions	Non-EU maritime administrations	Port State Control Officers	Other enforcement authorities	Public
Apply for a seafarer's certificate or endorsement	x		x						
Input the information required for the issue of a seafarer's certificate or endorsement	x	x	x						
Upload the supporting documents for the issue of a seafarer's certificate or endorsement	x	x	x						
View and edit the information on the seafarers	x	x							
Upload information on seagoing service	x								
Approve information on seagoing service			x						
Upload information on the training and education provided to seafarers	x	x			x				
Upload information on medical certificate	x	x		x					
Approve the application for a certificate or endorsement		x							
Issue a certificate or endorsement		x							
Verify the certificate or endorsement authenticity and validity	x	x	x	x	x	x	x	x	x

## ANNEX II Dataset

(Please refer to the excel file attached that shall be considered as an example and not as a complete or final version)



**European Maritime Safety Agency**

Praça Europa 4  
1249-206 Lisbon, Portugal  
Tel +351 21 1209 200  
Fax +351 21 1209 210  
[emsa.europa.eu](http://emsa.europa.eu)

