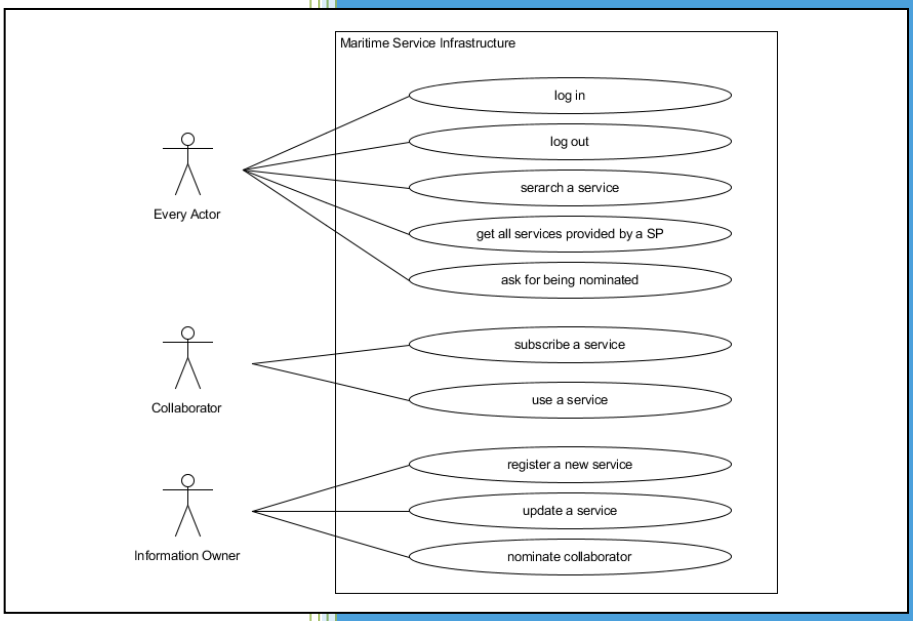
STM_Validation_D4.17
Analytical report describing technical service demand on STM services
2016-03-17



Co-financed by the Connecting Europe Facility of the European Union

DOCUMENT STATUS

Authors

Name	Organisation
Oliver Norkus	University of Oldenburg
Mikael Lind	Viktoria
Sandra Haraldsson	Viktoria

Review

Name	Organisation
Björn Andreasson	Swedish Maritime Administration
Cilli Sobiech	Viktoria
Michael Siegel	OFFIS

Approval

Name	Organisation	Signature	Date

Document History

Version	Date	Status	Initials	Description
0.01-0.3	Nov. + Dec. 2015	Initial	ON	Initial document
0.3	Dec 2015	Draft	ON	Shared with STM partners
0.4	Jan 2016	Draft	ON	Including Feedback on v0.3.. shared with STM partners
0.5	Feb 2016	Darft	ON	Including Feedback on v0.4.
0.6	14.03.201	Draft	ON	Including more use cases from Act 1 and 2
0.7	16.03.	Draft	ON	Include more feedback from Act 1, 2 and 4

TEN-T PROJECT NO: 2014-EU-TM-0206-S

The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained therein.

Table of contents

1 General Information

This document presents use cases for the digital infrastructure requirements within the Sea Traffic Management (STM) project. The use-case methodology is a tool for bridging the gaps between different domain experts and their perspectives. The objective with using the use-case methodology for the STM project is to provide a common structure to describe the large maritime system that STM encompasses. The structure will, thus, facilitate the iterative process of use-case development throughout the project.

Based on the use cases and the document “SeaSWIM Requirement Specification based on needs from PortCDM and Voyage Management_ver10”, requirements have been derived. Here the Requirements Abstraction Model (RAM) is applied. This model provides a way to describe requirements on an appropriate level and aims to reach a common understanding.

This introduction briefly describes what a use case is (see 1.1), with which the template the use cases are described here (see 1.2), what the RAM is (see 1.3) and which sources were used to discover the use cases and the requirements (see 1.4).

1.1 What is a use case?

Each Use Case describes a single scenario, business goal or task. Therefore, typically many Use Cases are needed to cover all scenarios for a particular system. All domain experts who will be impacted or will impact the system need to describe their own requirements through one or more Use Cases.

Use Cases treat the technology aspects of the system as a black box. Domain experts should describe the interrelation with the “black box” system from outside the system. This is a deliberate policy, because it simplifies the description of requirements, and avoid the trap of making assumptions about how this functionality will be accomplished. In other words, Use Cases capture the “what” of user requirements, but deliberately avoid addressing the “how” of technologies.

Developing Use Cases is both a science and an art. Domain experts need to follow the basic rules of Use Case development, but the degree of formality and details of a particular Use Case can vary significantly, depending upon whether the Use Case reflects relatively standard requirements or very new requirements, whether certain requirements are very stringent or rather loose, the relative importance of the particular Use Case within the complete set of Use Cases, and other factors. The key is to include enough details in the Use Cases; ensuring the user that the real needs are included, but not too many details so the result is overwhelming or confusing. Normal text…

1.2 Use case template

The Use Case template is used to describe the user requirements in the manner needed by the use case process. Here an adopted use case template based on the standard IEC 62559 is proposed to use as it is well suited. The template will be filled out for each use case.

Here is the annotated template in tabular form:

Table 1: use case template

UC_ID	Unique identification number	
Name	Name	
Origin	Provenance and origin	
Scope	Definition of goals and limits of the use case	
Objectives	ID	Description
	UC1_O1	List of targets and results to be achieved
	UC1_O2	
	UC1_O3	
Narrative	Full description from the user's perspective; Clarifies what and when is happening and why, with which purpose and under which conditions.	

Assumptions	General assumptions and prerequisites, and general remarks
Prerequisites	
General remarks	

Actors			
ID	Name	Type	Description
UC1_A1			

Scenarios					
ID	Name	Actor	Triggering event	Pre-condition	Post-condition

Steps for Scenario:		
Step-No.	Event	Description

1.3 Requirements Abstraction Model

This Requirement Abstraction Model (RAM) provides a way to describe requirements on an appropriate level depending on the audience. The purpose is to avoid the common misunderstanding that comes from discussing one certain issue on different levels and to allow requirements to be traced from a detailed component level to a more general goal level.

Very briefly the model goes from the most general description level “Product” (why) through “Feature” that is supported by the Product to “Function” (what it is supposed to do) and “Component” (how it is supposed to do it). More information can be found in this article Gorschek (2006) (DOI 10.1007/s00766-005-0020-7).

This model should be applied in the further refinement and specification process.

1.4 Origin, history and general notes

The use cases and requirements have been extracted from different documents and are the result of several meetings on this topic by STM partners especially Act4 and STM Vendors (associated to the project).

Especially, requirements have been taken from the initial requirements document within the STM project “SeaSWIM Requirement Specification based on needs from PortCDM and Voyage Management_ver10” as well as from documents of previous projects and projects with intersections. Here especially the document “Deliverable 3.1 Analysis Report” has to be mentioned as an outcome of the EfficienSea 2 project which provides a consolidated list of needs.

This document is a working document that is constantly filled and processed by Act 4. Prioritization of requirements is not listed in this document and still needs to be supplemented. In addition to the use cases and requirements, this document already generates initial design considerations.

Basic requirements for the target architecture are available. From this base, initial Use Cases have been derived and are described in this document. Therefore, this document mainly represents a general specification of Use Cases for Services in the Maritime Context.

This document is not a complete list of all STM use cases nor a complete list of Act4 use cases and requirements. It just provides some general use cases in the areas of unique identifiers, authentication, access management and service discoverability as core requirements within Act 4. As mentioned above, this document is a working document that is constantly filled and processed.

2 Use Cases

One of the most critical factors for the success of STM is that the data providers (information owners) have a low entrance barrier to the STM system. This means that even with limited access to IT resources it should be straightforward to make data sources available.

A data provider publishes information within a service and decides who has access to this data. For the consumption of data, a user has to ask for permission first.

With this permission, the one is becoming a collaborator who is authorized to use the service.

Here is an overview of the use cases:

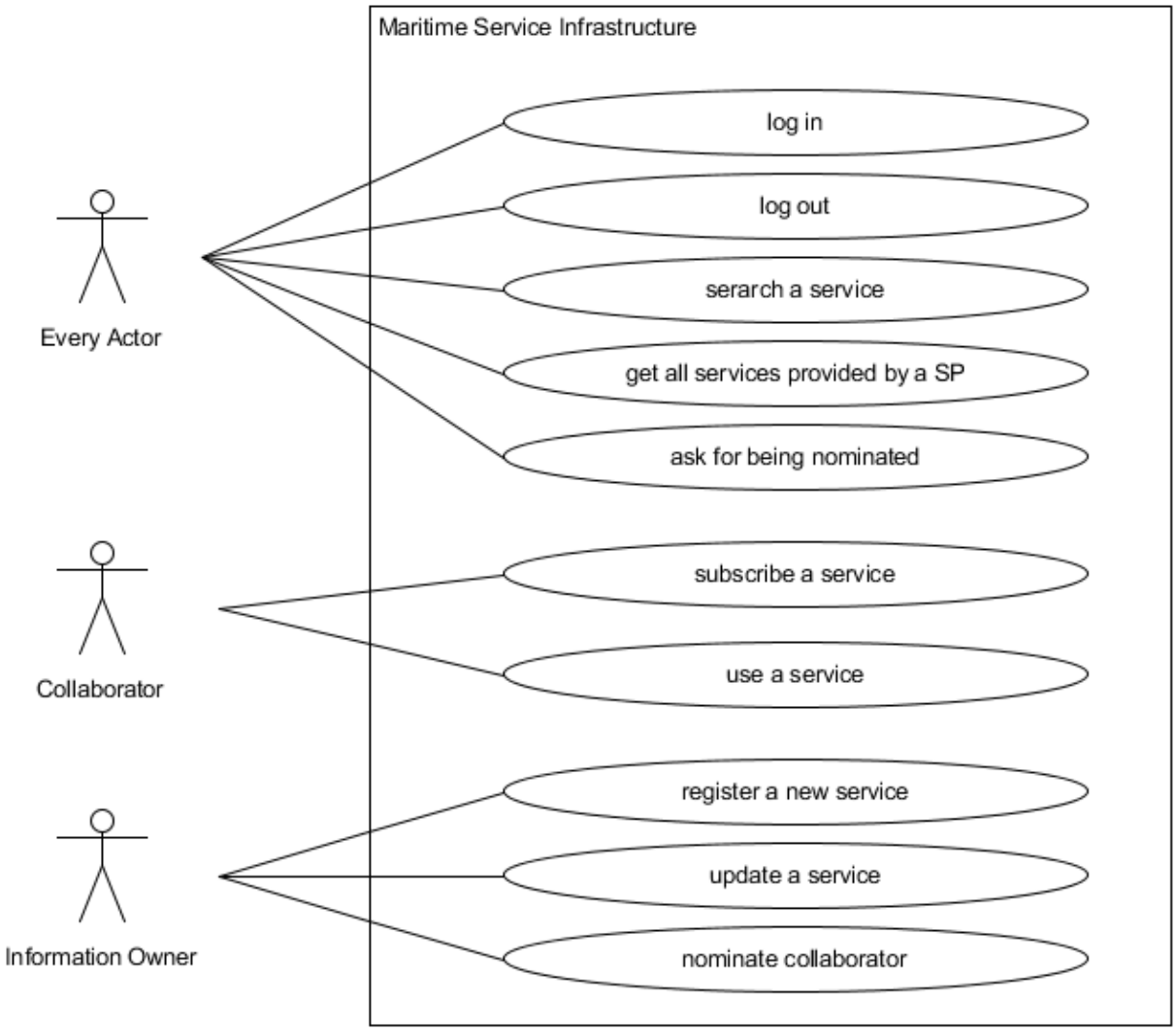


Figure 1: Use cases overview

2.1 STM_UC#1: Log in / out

UC_ID	STM_UC#1	
Name	Log in	
Origin	STM Req. #1, STM Req. #2	
Scope	The system shall ensure actors are who they claim to be.	
Objectives	ID	Description
	UC1_O1	User authenticated
	UC1_O2	Session opened
	UC1_O3	Session ID assigned
Narrative	The user has to authenticate himself. So to confirm, that he is known to the system and the system can uniquely identify the user.	

Assumptions	All items of identities must be identifiable.
Prerequisites	The user already got his access credentials.
General remarks	For the purpose of the STM project, it could be assumed that username/password authentication would be sufficient, but an evaluation of the risk and impact of a security breach should be conducted, to determine the realistic security policy to apply. In any case, foreseeing more than one assurance level should be considered. Facebook / google / linkedin logins could be suitable and easily provide a low level assurance login, but a higher level of assurance should most likely be applied.

Actors			
ID	Name	Type	Description
UC1_A1	User	Human	User who is going to log in
UC1_A2	Authentication Component	Identity Register	System checks the user's access credentials

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC1_S1	Passed	User clicks on button "Log in"	User has entered correct access credentials	User will be logged in, gets informed about the success
UC1_S2	Denied	User clicks on button "Log in"	User has entered incorrect access credentials	User is not logged in and informed about the mistrial

Steps for Scenario:		UC1_S1 Passed
Step-No.	Event	Description

UC1_S1_S1	User visits Log In Page	User enters his credentials
UC1_S1_S2	User clicks Log in	System checks the user credentials
UC1_S1_S3	Check positive	User credentials were correct, User will be logged in

Steps for Scenario:		UC1_S2 Denied
Step-No.	Event	Description
UC1_S1_S1	User visits Log In Page	User enters his credentials
UC1_S1_S2	User clicks Log in	System checks the user credentials
UC1_S1_S3	Check negative	User credentials were not correct, User will not be logged in. (Potentially offer mechanism to contact administrator or have credentials reset through secure process)

The Use Case “Log out” closes the established session. This use case is not considered in detail here.

2.2 STM_UC#2: Search a service

UC_ID	STM_UC#2	
Name	Search a service	
Origin	STM Req. #4	
Scope	A user searches for a service	
Objectives	ID	Description
	UC2_O1	Based on the parameters of a service, the service can be searched
	UC2_O2	The user matching to the search is displayed
	UC2_O3	
Narrative	The user has a need for a solution so he is looking for the matching service. Thereby, he searches for a service name or its description	

Assumptions	Any authenticated user may make the search for a service based on meta information.
Prerequisites	The user is authenticated. Standardized language for describing services.
General remarks	

Actors			
ID	Name	Type	Description
UC2_A1	User	Human	User searching for a service
UC2_A2	Search component	Service Registry	Search algorithm

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC2_S1	found	Search is to be executed	Search parameter(s) is entered	Result (service profile) is shown
UC2_S2	Not found	Search is to be executed	Search parameter(s) is entered	Absence of the searched service is reported

Steps for Scenario:		UC2_S1 Found
Step-No.	Event	Description
UC2_S1_S1	Search page is opened	Search parameter entered
UC2_S1_S2	Search button is clicked	Search algorithm runs, system scans the service registry
UC2_S1_S3	Search object found	Search object is displayed / List of matching services is displayed.

Steps for Scenario:		UC2_S2 Not Found
Step-No.	Event	Description
UC2_S2_S1	Search page is opened	Search parameter entered
UC2_S2_S2	Search button is clicked	Search algorithm runs, system scans the service registry
UC2_S2_S3	Search object not found	Inform user of the negative result of the search

2.3 STM_UC#3: Get all services provided by a Service Provider

UC_ID	STM_UC3	
Name	Get all services provided by a Service Provider	
Origin	STM Req. #4	
Scope	A user wants to get a list of all services provided by a concrete Service Provider.	
Objectives	ID	Description
	UC3_O1	The services offered by a specific provider be determined and displayed.
	UC3_O2	
	UC3_O3	
Narrative	A ship is on its way to a port. The captain wants to know the port and the service providers, and therefore he wants to see all the services offered.	

Assumptions	Any authenticated user may search for a service list of a specific service provider.
Prerequisites	The user is authenticated.
General remarks	

Actors			
ID	Name	Type	Description
UC3_A1	User	Human	User willing to see the list of services provided by a specific service provider.
UC3_A2	Search component	Service Registry	Search algorithm within the service registry

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC3_S1	found	Search is to be executed	Service Provider's name is entered	List of services is shown
UC3_S2	Not found	Search is to be executed	Search parameter(s) is entered	Error message is shown

Steps for Scenario:		UC3_S1 Found
Step-No.	Event	Description
UC3_S1_S1	Search page is opened	The user visits the search page of the service registry. He enters the name or description of the service provider.
UC3_S1_S2	Search button is clicked	The search engine of the service registry is operating to get the list of all services provided by the service provider.
UC3_S1_S3	Search objects found	The list of the services is determined. The user gets the list of services.

Steps for Scenario:		UC2_S2 Not Found
Step-No.	Event	Description
UC3_S2_S1	Search page is opened	The user visits the search page of the service registry. He enters the name or description of the service provider.
UC3_S2_S2	Search button is clicked	The search engine of the service registry is operating to get the list of all services provided by the service provider.
UC3_S2_S3	Search object not found	Inform the user of the negative result of the search, whether the service provider cannot be found, or the list of services is empty.

2.4 STM_UC#4: Ask for being nominated

UC_ID	STM_UC#4	
Name	Ask for being nominated	
Origin	STM Req. #2	
Scope	A user wants to get the right to use a service.	
Objectives	ID	Description
	UC4_O1	A request for being nominated is created.
	UC4_O2	Request to get read access is sent to the information provider (owner).
	UC4_O3	The information provider receives the new request in his input channel.
Narrative	An authenticated user wishes to use a service and thus consume the information provided through the service. He has already found this service (e.g., via UC#2 or UC#3) and is currently not allowed to use the service due to a lack of appropriate permissions.	

Assumptions	Any authenticated user may make the search for a service based on meta information and can ask for being nominated.
Prerequisites	The user is authenticated. The user has already found the service. Currently the user does not have the right to use this service.
General remarks	

Actors			
ID	Name	Type	Description
UC4_A1	User	Human	User asking for the right of use
UC4_A2	Nomination Forwarding Component	Service Registry	Component within the service registry receives the request and forwards the request to the information owner.
UC4_A3	Nomination processing component	Service Provider	This component receives the request.

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC4_S1	Successful	Actor asks for being nominated.	User has found the service and wanted to use it.	The request was send to the information owner successfully.
UC4_S1	Not Successful	Actor asks for being nominated.	User has found the service and wanted to use it.	No request made.

Steps for Scenario:		UC4_S1
Step-No.	Event	Description

UC4_S1_S1	User is willing to ask for being nominated.	The user sees meta information of the service and is willing to access the information by using the service.
UC4_S1_S2	User clicks on “ask for access”	System receives the request and forwards the request to the information owner. An acknowledgment of receipt is available. The information owner decides on the nomination (see UC#9).
UC4_S1_S3	Request sent	User is informed that the request is successfully send to the information provider namely to the nomination processing component.

Steps for Scenario:		UC4_S2
Step-No.	Event	Description
UC4_S2_S1	User is willing to ask for being nominated.	The user sees meta information of the service and is willing to access the information by using the service.
UC4_S2_S2	User clicks on “ask for access”	System does not receive the request or and forwards the request to the information owner, but an acknowledgment of receipt is not available.
UC4_S2_S2	Error information	User gets informed, that the request is not successfully send to the information provider.

2.5 STM_UC#5: Subscribe a service

UC_ID	STM_UC#5	
Name	Subscribe a service	
Origin	STM Req. #5	
Scope	A user wants to get automatically updated information delivered by a service. The user subscribes this service.	
Objectives	ID	Description
	UC5_O1	User is a registered subscriber of this service
	UC5_O2	The service sends (pushes) new information automatically to the user
	UC5_O3	
Narrative		

Assumptions	
Prerequisites	The user is authenticated. The user has already been nominated to use this service. Otherwise, it has to be done first. The service provider offers the subscription function for this service.
General remarks	

Actors			
ID	Name	Type	Description
UC5_A1	User	Human	
UC5_A2	Subscription forwarding component	Service Registry	Component within the service registry forwarding the request to the subscription processing component on the side of the service provider.
UC5_A3	Subscription processing component	Service Provider	Component within the service provider, receives the request, adds the user to the subscribers list and sends a confirmation to the user.

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC5_S1	Successful	User clicks on “subscribe”	User is allowed to consume the service	The user gets automatically updated information from the service.
UC5_S2	Not successful	User clicks on “subscribe”	User is not allowed to consume the service	The user gets the information that the subscription does not work

Steps for Scenario:		UC5_S1 Successful subscription
Step-No.	Event	Description
UC5_S1_S1	User clicks on “subscribe”	User wants to subscribe to this service. He clicks on the button “subscribe”. The service registry component “subscription forwarding” sends the request to the “subscription processing component” or to the service provider.
UC5_S1_S2	Subscription confirmed	“Subscription processing component” accepts the request, adds the user to the subscription list.
UC5_S1_S3	User informed	The user gets informed that he is now on the list of subscribers.

Steps for Scenario:		UC5_S2 Subscription not successful
Step-No.	Event	Description
UC5_S1_S1	User clicks on “subscribe”	User wants to subscribe to this service. He clicks on the button “subscribe”. The service registry component “subscription forwarding” sends the request to the “subscription processing component” or to the service provider.
UC5_S1_S2	Subscription not confirmed	“Subscription processing component” does not receive or accept the request, the user is not added to the subscription list.
UC5_S1_S3	User informed	The user gets informed what went wrong.

2.6 STM_UC#6: Use a service

From the viewpoint of a central SeaSWIM architecture, the concrete use cases describing the usage of services and application services are part of the other activities in the STM project (Act1/Act2). In this document, the focus lays on the SeaSWIM aspects, the derived requirements and related use cases. But, to get a concrete idea what kind and type of application services could be used, here we outline a few use cases from Act 1 and Act 2.

2.6.1 STM Act 2 Voyage Management use cases

2.6.1.1 STM_UC#6.1 Voyage Management: Route optimization

UC_ID	UC#6.1	
Name	Route optimization	
Origin	STM Act 2 Voyage Management	
Scope		
Objectives	ID	Description
	UC1_O1	
	UC1_O2	
	UC1_O3	
Narrative	The route optimization tools will be different in nature with a common purpose to provide more information for the navigator on board. The STM concept will provide the means to get the ships route optimized from different service providers. The service providers have different foci including best route regarding: weather forecast, surface currents, fuel consumption, no-go areas, areas with sensitive nature, conflicts with other ships routes etc.	

Assumptions	
Prerequisites	Actor is nominated and allowed to use the route optimization service. All information needed for this case are available.
General remarks	Testbed usage: Ships participating in the test beds will be offered to take part of the route optimization services that are developed within the STM project. In the test bed “rtz” format is used and ships identification/UVID is also required. Other information needs than these needs to be transferred by other means. Different attributes needed for different optimization services. No standard format exists.

Actors			
ID	Name	Type	Description
UC1_A1			

Scenarios					
ID	Name	Actor	Triggering event	Pre-condition	Post-condition
1	Service provider wants to provide route optimization service	Service provider	Register a new service	Service description template is fulfilled with all relevant meta information for this service	New route optimization service is available in the registry and is discoverable
2	Vessel operator is looking for an optimization service	Navigator on board / Vessel	Searching a service	Service is discoverable	Service found
3	Vessel operator uses the route optimization service	Navigator on board	Vessel request optimization	Definition/Specification of SeaSWIM connector/Voyage	Navigator has received the optimized route

Steps for Scenario		1 - Service provider wants to provide route optimization service
Step-No.	Event	Description and data flow
1.1	Register service	The service provider uploads a new service description to the service registry.
1.2	Registration confirmed	Service Registry sends a confirmation to the service provider
1.3	Nominate actors	The service provider nominates a list of actors which are allowed to use the service. The service management on the service providers' side adds the actors to the access control list.
1.4	Nomination confirmed	The nomination service confirmed the nomination.

Steps for Scenario:		2 - Vessel operator is looking for an optimization service
Step-No.	Event	Description and data flow
2.1	Identification Oneself	Vessel identifies itself in the SeaSWIM environment by log in.
2.2	Authentication	Log in confirmed, Actor is authenticated.
2.3	Discover Service	Operator goes to Service Registry Website and asks for related services

2.4	Check if authorized	The service registry checks if the actor is authenticated.
2.5	Confirmation	ID Registry confirms the identity of the actor
2.6	List of services	Service Registry delivers a list of relevant services to the authenticated actor.

Steps for Scenario:		3 - Vessel operator uses the route optimization service
Step-No.	Event	Description and data flow
3.1	Vessel requests optimization	Navigator on boards has decided to use this service and now sends a route optimization request to a route optimization service.
3.2	Authorization check	Service checks the caller's authorization
3.3	Authorization confirmed	Nomination service confirms that the actors is allowed to use the service
3.4	service confirms readiness	Service is accessible and available and confirmed willingness to work. Service instructs the requesting component to send the relevant data.
3.5	Vessel provides data	The vessel provides all relevant data to the route optimization service. Service provider receives voyage plan to be optimized. This could be done by a push or a pull mechanism – for details see Use Case Description within Activity 2 Voyage Management.
3.6	Optimized route send to vessel	The route optimization has received the voyage plan (VP) and has performed the optimization. The result is send to the vessel. The optimized route is made available for the ship by sending the ".rtz" file to the vessel.
3.7	Vessel confirms the reception	Optimized VP is available at the vessel.
3.8	Vessel decides on suggested route	When/If an optimized route suggestion is loaded for monitoring, all actors with access rights shall be notified that a new voyage plan is available
3.9	Vessel accepted route and sends confirmation	Route optimization service provider should get (automatic) acknowledgement when optimized route is installed at the onboard system, not that operator has seen suggestion.

2.6.1.2 STM_UC#6.2 Voyage Management: Route Cross-check

UC_ID	6.2	
Name	Route cross-check	
Origin	STM Act 2 Voyage Management	
Scope		
Objectives	ID	Description
	UC1_O1	
	UC1_O2	

	UC1_O3	
Narrative	The intended voyage plan is sent to a shore based service provider for cross-checking. The purpose is to include updated regional area information that could affect the ship´s voyage plan. The cross-checking can be done before the vessels departure or before arrival at a certain geographical area. The cross-check can include, but is not limited to, Under Keel Clearance (UKC), air draught, no violation of no-go areas, Maritime Service Infrastructure (#MSI) and compliance with mandatory routing. No optimization service as such is included in the route validation.	

Assumptions	
Prerequisites	The service is available in the service registry and the actor is nominated and allowed to use the route cross check service according to Scenario 1 Route optimization. All information needed for this case are available. Ship/vessel operator finds service in the service registry according to Scenario 2 Route optimization
General remarks	Testbed usage: In the test beds shore centers will act as the service providers performing route cross-checking. The cross-checking will be limited to the shore centers area of responsibility. Operators in the shore centers can be supported by software when performing the route cross check.

Actors			
ID	Name	Type	Description
UC1_A1			

Scenarios					
ID	Name	Actor	Triggering event	Pre-condition	Post-condition
1	Route cross check service			Shore centers check route and send back confirmation or new proposal (might include text message)	

Steps for Scenario:		2 – Route cross check service
Step-No.	Event	Description and data flow
1	Ship requests a route Cross-Check	Navigator on boards has decided to use this service and sends a request to a Route cross check service.
2	Authorization check	Service checks the caller's authorization (not necessary for test bed)
3	Authorization confirmed	Nomination service confirms that the actors is allowed to use the service (not necessary for test bed)

4	Service confirms readiness	Service is accessible and available and confirmed willingness to work. Service instructs the requesting component to send the relevant data.
5	Vessel sends data	The vessel sends all relevant data to the route cross check service. Service provider receives voyage plan to be checked. In the test bed “rtz” format is used and ships identification/UVID is also required.
6	Optimized route send to vessel	The shore center (SC) has received the voyage plan and has performed the cross check. SC should be able to confirm to the ship that the route is checked and ok (route status 4 according to route flow chart) or alternatively send a route suggestion (new voyage plan).
7	Acknowledgement SC checked route reaches the ship	SC should get (automatic) acknowledgement when the ok/suggested VP is available at the onboard system (delivered onboard, not that operator has seen suggestion).
8	Ship accepts or rejects suggested route	When/If a new route suggestion is loaded for monitoring all actors with access rights shall be notified that a new voyage plan is available

2.6.1.3 STM_UC#6.3 Voyage Management: Enhanced Monitoring

UC_ID	6.3	
Name	Enhanced monitoring	
Origin	STM Act 2 Voyage Management	
Scope		
Objectives	ID	Description
	UC1_O1	
	UC1_O2	
	UC1_O3	
Narrative	Enhanced monitoring will be supported by adding route information and a monitoring service can be provided in previously unmonitored areas. Shore centres will be able to detect if the planned schedule is not kept or if a ship deviates from the planned route. Thus shore centres can monitor that ships are following their planned route and also foresee possible dangerous situations and suggest route modifications (geographic and/or speed) due to traffic or other impeding conditions. These tools can also enhance current VTS services.	

Assumptions	
Prerequisites	Actor is nominated and allowed to use the enhanced monitoring service. All information needed for this case are available.
General remarks	Testbed usage: The shore centres should exchange routes with the ships (send and receive routes/route segments) ship to shore via MDI (SWIM connector) and display them on the VTS/STM shore centre system. All STM ships within predefined areas (AIS coverage limitation due to input of pos, course etc.), from shore centre will be

	monitored from shore centre. The shore centre operators will be supported by anomaly detection tools, described elsewhere, to be taken into operation in the project. TCP/IP based exchange of navigational data via new message format/extension to other format will be tested on some ships.

Actors			
ID	Name	Type	Description
UC1_A1			

Scenarios					
ID	Name	Actor	Triggering event	Pre-condition	Post-condition
1	Service provider wants to provide enhanced monitoring service	Service provider	Register a new service	Service description template is fulfilled with all relevant meta information for this service	New enhanced monitoring service is available in the registry and is discoverable
2	Vessel operator is looking for an enhanced monitoring service	Navigator on board / Vessel	Searching a service	Service is discoverable	Service found
3	Vessel operator uses the enhanced monitoring service	Navigator on board	Vessel request enhanced monitoring	Definition/Specification of SeaSWIM connector/Voyage	Ship will be monitored by designated shore centre

Steps for Scenario:		1 - Service provider wants to provide enhanced monitoring service
Step-No.	Event	Description and data flow
1.1	Register service	The service provider uploads a new service description to the service registry.
1.2	Registration confirmed	Service Registry sends a confirmation to the service provider

1.3	Nominate actors	The service provider nominates a list of actors which are allowed to use the service. The service management on the service providers' side adds the actors to the access control list.
1.4	Nomination confirmed	The nomination service confirmed the nomination.

Steps for Scenario:		2 - Vessel operator is looking for an enhanced monitoring service
Step-No.	Event	Description and data flow
2.1	Identification Oneself	Vessel identifies oneself in the SeaSWIM environment by log in.
2.2	Authentication	Log in confirmed, Actor is authenticated.
2.3	Discover Service	Operator goes to Service Registry Website and asks for related services
2.4	Check if authorized	The service registry checks if the actor is authenticated.
2.5	Confirmation	ID Registry confirms the identity of the actor
2.6	List of services	Service Registry delivers a list with relevant services to the authenticated actor.

Steps for Scenario:		3 - Vessel operator uses the enhanced monitoring service
Step-No.	Event	Description and data flow
3.1	Vessel requests Enhanced monitoring service	Navigator on boards has decided to use this service and now sends a request to an Enhanced monitoring service.
3.2	Authorization check	Service checks the caller's authorization
3.3	Authorization confirmed	Nomination service confirms that the actors is allowed to use the service
3.4	Service confirms readiness	Service is accessible and available and confirmed willingness to work. Service instructs the requesting component to send the relevant data.
3.5	Vessel sends data	The vessel sends all relevant data to the Enhanced monitoring service. The information needed are: AIS (Needed for actually monitor the vessel, not for sending via SeaSWIM) .rtz The format ".rtz" is used. Service provider receives voyage plan to be Enhanced monitored.
3.6	Ship enters the Enhanced monitoring services monitored area and Enhanced	The Enhanced monitoring service has received the route data and performs Enhanced monitoring. Enhanced monitoring service to inform the vessel that the Enhanced monitoring service is commenced

	Monitoring is commenced	
3.7	Ship confirms that Enhanced monitoring is Commenced	Ship receives information from Enhanced monitoring service that Enhanced monitoring is commenced and confirms back to Enhanced monitoring service.

2.6.2 STM Act 1 PortCDM use case scenarios

Act 1 PortCDM does not fill out the template completely. Therefore, here is just an overview of possible scenarios illustrated. Possible further scenarios are not explicitly described here.

ID	Name	Actor	Triggering event	Precondition	Postcondition
1	Vessel informs port about ETA, PTA	Vessel	Port Call as part of the voyage plan	Subscription services forthcoming port call	Foundations created for port call synchronization
2	Port actors provide info about plans and outcomes	Port actor	A state change by any port call actor	SeaSWIM connectors calling the PortCDM state update service	Instantiated port call process (first time) and time stamps related
3	Port call actors consume PortCDM informations	Port call actor	A port call actor supplies time stamp	Nomination schemas and nomination services and discoverable PortCDM services	PortCDM service consumed by port call actors

2.7 STM_UC#7: Register a new service

UC_ID	STM_UC7	
Name	Register a new service	
Origin	STM Req. #4, #5	
Scope	New information to be provided	
Objectives	ID	Description
	UC7_O1	The information (the new service) should be available and discoverable after uploading
	UC7_O2	
	UC7_O3	
Narrative	Publish the availability of new information.	

Assumptions	1) Stakeholders are willing to share data/information. 2) Other stakeholders find the shared data/information useful to improve their operations.

Prerequisites	1) Commonly known standards for the information. 2) Known interfaces to reach the information. 3) Available servers and databases where the information resides.
General remarks	There has to be a place to upload meta data too.

Actors			
ID	Name	Type	Description
UC7_A1	Information Owner	Human	A user in the role Information Owner wants to publicize the availability of their new information
UC7_A2	Service Repository	System	Gets the information regarding the new service accessible via the service registry

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC7_S1	Successful	Upload service meta data to service register	Information Owner wants to add a new service	New discoverable service in the service register
UC7_S2	Not successful	Upload service meta data to service register	Information Owner wants to add a new service	Error message, service to be uploaded is not in the service register yet

Steps for Scenario:		UC7_S1 Successful
Step-No.	Event	Description
UC7_S1_S1	Meta data upload	Information Owner uploads the description of the new service
UC7_S1_S2	Store meta data	Information Owner clicks the “save” button
UC7_S1_S3	Added service	The availability of a new service is now stored in the service register
UC7_S1_S4	Confirmation	Information Owner gets positive feedback from the registry

2.8 STM_UC#8: Update a service

UC_ID	STM_UC#8	
Name	Change meta information of a service	
Origin	STM Req. #4, #5	
Scope	An information owner (provider) wants to change the meta information of an information.	
Objectives	ID	Description
	UC8_O1	Metadata was changed successfully
	UC8_O2	
	UC8_O3	

Narrative	The Information Owner is willing to update the meta data of a service stored in the service register.

Assumptions	Only the information owner can update the service.
Prerequisites	1) Commonly known standards for the information. 2) Known interfaces to reach the information. 3) Available servers and databases where the information resides.
General remarks	

Actors			
ID	Name	Type	Description
UC8_A1	Information Owner	Human	
UC8_A2	Service registry	System	

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC8_S1	Successful	Updated meta data	Information Owner wants to update an existing service	Updated service is discoverable.
UC8_S2	Not successful	Updated meta data	Information Owner wants to update an existing service	Error message, service not updated.

Steps for Scenario:		UC8_S1
Step-No.	Event	Description
UC8_S1_S1	Meta data upload	Information Owner uploads the new description of the new service
UC8_S1_S2	Store meta data	Information Owner clicks the “save” button
UC8_S1_S3	Updated service	The updated service description is now stored in the service registry.
UC8_S1_S4	Confirmation	Information Owner gets positive feedback from the registry

2.9 STM_UC#9: Nominate collaborator

UC_ID	STM_UC#9	
Name	Give access for a user to the information provided by the service	
Origin	STM Req. #2	
Scope	The information owner wants to provide access to a specific user/group, geographical region, time window.	
Objectives	ID	Description
	UC9_O1	The user who requested the read access can now read this information (use the service).
	UC9_O2	
	UC9_O3	
Narrative	A potential information consumer has requested to being nominated regarding a specific service. The information provider (owner) get the request and grant the read access.	

Assumptions	
Prerequisites	Request to being nominated exists (see UC#4)
General remarks	

Actors			
ID	Name	Type	Description
UC9_A1	Information Owner	Human	
UC9_A2	Nomination processing component	Service Provider	

Scenarios				
ID	Name	Triggering event	Pre-condition	Post-condition
UC9_S1	Access granted	Request of being nominated is to be processed now	STM_UC2	answered request, access is allowed
UC9_S2	Error	Request of being nominated is to be processed now *Same like above, one scenario with tree endpoints*	STM_UC2	Read access changed not successful, system error
UC9_S3	Access denied	Request of being nominated is to be processed now	STM_UC2	answered request, access is not allowed

		Same like above, one scenario with tree endpoints		

Steps for Scenario:		UC9_S1 Access granted
Step-No.	Event	Description
UC9_S1_S1	Information Owner will handle the nomination request	Information owners looks at the requesting user, examines whether an NDA is required and present.
UC9_S1_S2	Information Owner clicks on “Nominate the user”	Information Owner decides positive regarding the right of access.
UC9_S1_S3	Adding the new user to the ACL	The System adds the user to the Access Control List.
UC9_S1_S4	Information Owner clicked on “save”	success confirmation to the requesting user (the new collaborator)

Steps for Scenario:		UC6_S2 Error
Step-No.	Event	Description
UC9_S2_S1	Information Owner will handle the nomination request	Some system errors, Error message

Steps for Scenario:		UC6_S3 Access denied
Step-No.	Event	Description
UC9_S3_S1	Information Owner will handle the nomination request	Information owners looks at the requesting user, examines whether an NDA is required and present.
UC9_S3_S2	Information Owner clicks on “Not nominate the user”	Information Owner decides negative regarding the right of access. Information forwarded to the requesting user (not becoming a new collaborator)

3 Requirements Identification

Based on the use cases and the preexisting documents, the following requirements were identified. They are refined and discussed in the next section. Here, a list and description of their origin.

Orgin Req. No.	Description
#1	Unique Voyage ID
#1, #2, #4	Reliable service identifiers
#1, #2, #4	Reliable user identifiers
#4	Discoverability of services
#4, #5	Common, standardized service description language
#4	Discoverability of identities
#1.1	Global (distributed) identity registry
#1.2	Global (distributed) service registry
#2	Access Control
#2.1	Information Owner access control
#2.2	Information Owner access nomination
#3, #1	Reliable P2P over multiple communication channels
#3, #2	Secure P2P over multiple communication channels
#5	Push based interaction (subscription)
#5	Pull based interaction
#5	Broadcast based interaction
#8	Logging based interaction
#10	3rd party development
#12	Non-standardized message interaction
#6, #1	Integrated, common data model
#6, #2	Data quality and versioning
#7	STM message standard (intentions and states)
#11	Status of communication (received, agreed, implemented etc.)
#10	Service portfolio management
#9	Monitoring and evaluate service provision and consumption
#9	Usage-based billing model

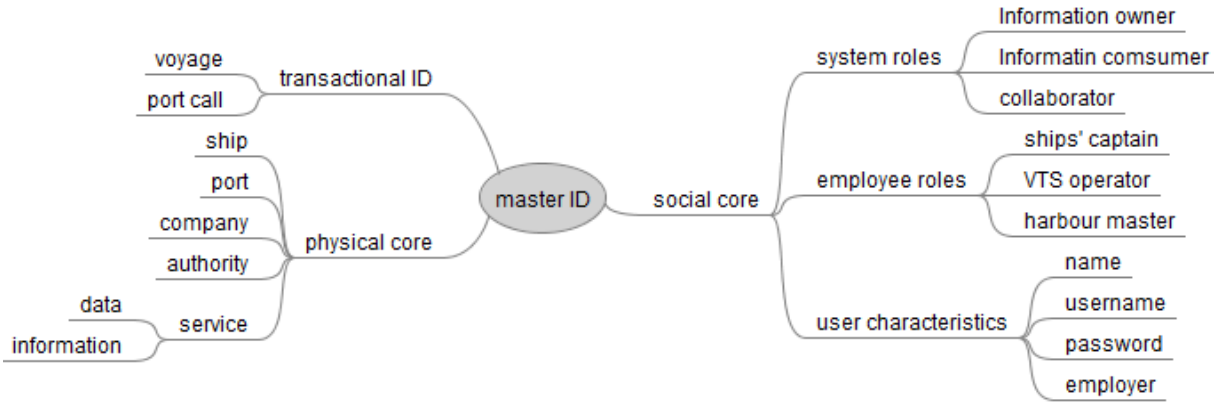
4 Refinement of Requirements

Based on the use cases and requirement identification the system requirements are refined and discussed in the following sections.

4.1 Identity management and role-based access control

(1) All types and attributes of identities must be identifiable.

The following illustration gives an overview of identity types and hierarchical structure.



(2) A Universal Identifier for all identities is needed. The UID concept must be flexible, decentralized, and forward compatible.
(3) An ID registry is needed, which can uniquely identify all identity entities and facilitate lookup of secondary identifying attributes.
(4) Identities shall be discoverable based on different criteria.
(5) A user-role concept is needed. A user can hold multiple roles.
(6) Standardized functions for authentication of identities and validation of authenticity is needed.
(7) Standardized functions for authorization is needed.
(8) Ownership of information elements and authorization to pass it on, must be managed

4.2 Service definition, discoverability and interactions

(1) The system shall provide a Service Registry and a look up function.
(2) Services should be grouped together (Cluster). For instance, clusters can be platform specific, add-on services or a geographical subset.
(3) Different types of service interactions shall be implemented.
    a. Push types based on a subscribe interaction. Standardized methods for setting up a subscription to a service should be developed.
    b. Request-response type service based on a client's request. This type allows for distinguished (authenticated) clients.
    c. Broadcast type service to make information available for a group of clients, e.g. in a selected geographical area. This type does not allow for distinguished (authenticated) clients
(4) Services shall be discoverable based on different criteria.

(5) The usage of services shall be restrictable (e.g. restricted access from mobile actors requiring global location services)
(6) Extensibility: also third-party developers should be able to provide their services as a part of service portfolio management.

4.3 Service usage and information consumption

(1) Information should have a hierarchical structure.
(2) The system shall ensure that access to and provision of single information objects which exists in a larger information structure (data model). This is done in relation to the larger information structure.
(3) Access should be platform independent
(4) Access should be possible from all standard devices.

4.4 Security

(1) The system must provide standardized means to support the encryption of data.
(2) Versatile Point-to-Point (P2P) Information Transfer
    a. Reliable P2P information transfer despite different types and qualities of communication channels.
    b. Provide mechanisms to mitigate poor connectivity quality, thus relieving deployed services from that responsibility. This can, for instance, include store-and-forward mechanisms in the SeaSwim communication protocols.
    c. Support scalable payloads: At one extreme, due to slow and expensive connection on-board vessels, the overhead for communication must be kept at a minimum. At the other extreme, communication between land-based clients' needs to be fast, and may entail transfer of large amounts of data.
(3) Secure P2P information transfer
    a. Secure encrypted end to end connectivity
    b. Information shall be protected from unauthorized access in all communications

4.5 Messaging Service, communication, information access

(1) A messaging service shall be present.
(2) The messaging service should support the capability to broadcast information to actors inside an area or actors subscribing to information in an area or along a route.
(3) Dynamic Multicast groups for multicasting information only to actors related to a particular operation shall be present.
(4) A messaging service should support requesting acknowledgement of information delivery.
(5) Seamless roaming: Actors should be able to interact without using the same p-2-p radio link or the same satellite system. And to switch from one communication channel to another.

(6) The system shall facilitate ongoing real-time updates of information and shall be free of redundancies, i.e. all services have access to consistent information.
(7) The status of the communication shall be present and redistributable
(8) Text messages with non-standardised content shall be supported.

4.6 Monitoring and Management

(1) Access Log: All requests and changes should be logged
(2) The provisioning, the consumption and the quality of services shall be captured and monitored; access on this shall be continuously.
(3) Service consumer shall be able to evaluate their service usage in a quantitative and qualitative way (including rankings)
(4) Service providers should be informed about this review.
(5) Users shall be able to view the log files
(6) Users shall be able to analyse usage patterns.

5 Sorting Requirements with RAM

In this section a first draft of the sorting and categorisation of the requirements from the previous section is done.

Software (and hardware) components that will provide these functions are currently conceptualized in the architecture specification. To finalize the document a mapping 'function to component' is supplemented here.

Product	Req. No.	Feature	Subfeature	Function	Component
Flexibility	#1	Unique identities	Unique Voyage ID	Search identified entity	
Flexibility	#1, #2, #4	Reliable identities	Reliable service identifiers	Search service	
Flexibility	#1, #2, #4	Reliable identities	Reliable user identifiers	Search identified entity	
Flexibility	#4	Unique identities	Discoverability of services	Search service	
Flexibility	#4, #5	Data quality	Common, standardized service description language	Search identified entity, search service, use service	
Flexibility	#4	Unique identities	Discoverability of identities	Search identified entity	
Flexibility	#1.1	Unique identities	Global (distributed) identity registry	Search identified entity	
Flexibility	#1.2	Unique identities	Global (distributed) service registry	Search identified entity, search service, use service	
Security / Trust	#2.1	Access Management	Information Owner access control	Search identified entity, search service, use service	
Security / Trust	#2.2	Access Management	Information Owner access nomination	Search identified entity, search service, use service, Nomination service	
Security / Trust	#2.2	Access Management	Access control	Authorization check, Search identified entity, search service, use service, Nomination service	
Flexibility	#3, #1	Reliable communication	Reliable P2P over multiple communication channels	Every communication	
Security / Trust	#3, #2	Secure communication	Secure P2P over multiple communication channels	Every communication	
Flexibility	#5	Flexible service interactions	Push based interaction	subscription	

Flexibility	#5	Flexible service interactions	Pull based interaction	search service, use service	
Flexibility	#5	Flexible service interactions	Broadcast based interaction	automatic release	
Flexibility	#8	Flexible service interactions	Logging based interaction		
Flexibility	#10	Service Management	3rd party development	service portfolio enhancements	
Flexibility	#12	Flexible service interactions	Non-standardized message interaction		
Structure	#6, #1	Data quality	Integrated, common taxonomy		
Structure	#6, #2	Data quality	Data quality and versioning		
Structure	#7	Flexible service interactions	STM message standard (intentions and states)		
Structure	#11	Reliable communication	Status of communication (received, agreed, implemented etc.)	Every communication	
Security / Trust	#10	Service Management	Service portfolio management		
Analytics	#9	Monitoring	Monitoring and evaluate service provision and consumption	optimization	
Flexibility	#9	Accounting	Usage-based billing model	Billing	

6 Architectural Considerations

6.1 Actors, Identities and Access Management

An ACTOR in the use cases of this document represents *an Entity that need to interact with other Entities.* (Note that an Entity may have several Identities, used to represent the Entity as an ACTOR in a particular context.)

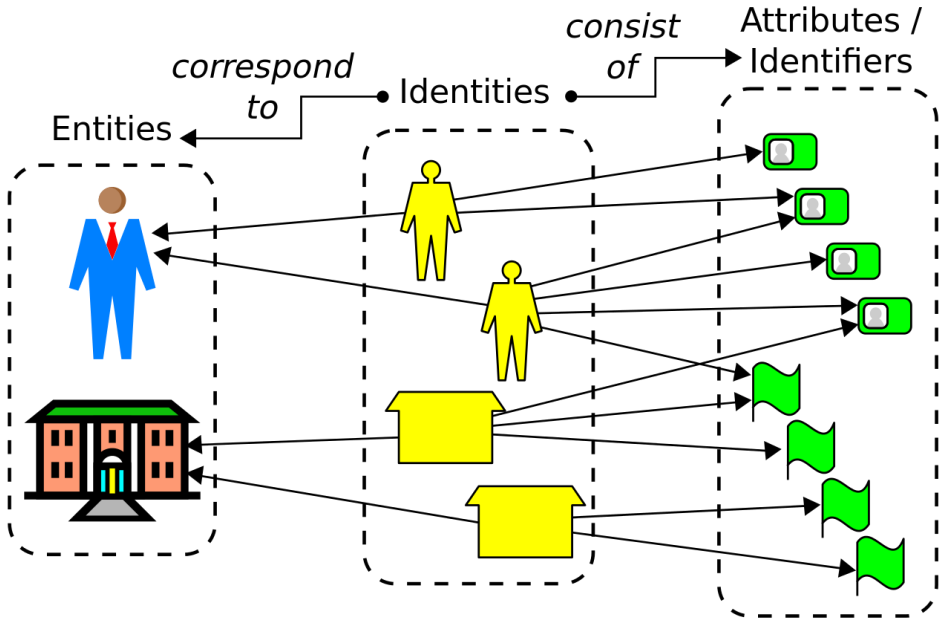


Figure 2: Relationship between Entities, Identities and Identifiers.

*(Source: **https://en.wikipedia.org/wiki/Identity_management)***

Digital transactions between Entities often require a certain level of trust in who the interaction takes place with. Actor Identities must therefore be *uniquely identifiable* by a Unique Identifier (UID), which is an Attribute that describe one unique ACTOR IDENTITY.

The process of confirming that an Identity is who it claims to be, is called *Authentication*. This is what happens when a user logs onto a system, and the system validates that the *credentials* (for instance username/password) actually match data only available to the right Entity, to a certain *Assurance Level*.

Different Assurance Levels may be required for different purposes. Low assurance levels may require nothing more than a self-registered username/password, high assurance levels may require two-factor authentication processes or inheritance factor validation difficult to fake.

NIST 800-63 is a guideline from National Institute of Standards and Technologies that describes four levels from “little or no confidence in the asserted identity” to “very high confidence in the asserted identity”. The European eIDAS regulation (http://ec.europa.eu/digital-agenda/en/trust-services-and-eid) define three assurance levels (low, substantial, high)

Example: In an internet banking system a low assurance level may be sufficient to give users easy access to check their bank account (low impact of security breach), but two factor authentication may be required to perform banking transactions (high impact of a security breach).

Actor Identities with a social core are denoted 'Users'. A User represents an individual (Ships captain, VTS operator, employee). Other Actor Identities may have a Physical or Logical core (Ship, Device, Service) or Organizational core (Port, Company, Authority).

Depending on the type of Actor, other Attributes may be used to classify or describe characteristics of an Identity, such as *name, username, e-mail, address, callsign, UNLOCODE*. While a UNLOCODE may help identify the location of a Port, it is not relevant to describe a User.

6.1.1 Access Management: Roles, Permissions and Constraints

Role-based access control (RBAC) is a common approach to restricting system access to authorized users.[1]

In RBAC, and Actor (or *subject*) can get a PERMISSION (to execute certain functions of services, like reading or writing data), only if the Actor has been assigned one or more ROLE(s).

The Role must be authorized for the Actor, and Roles may be authorized to exercise one or more Permissions.

In other words: If a User (and Actor) is assigned the Role as 'Information Owner', and the Role 'Information Owner' is authorized to exercise permissions *Read*, *Write*, *Modify* and *Delegate* in a service, then the User can access functions that require these permissions. If a User is assigned a Role as 'Consumer', and 'Consumer' is authorized with permission 'Read Only', then the User can only access and execute 'Read' functions.

Additional CONSTRAINTS may apply – for instance a restrictive rule on the potential inheritance of permissions from opposing roles, to achieve appropriate separation of duties. For example, the same person should not be allowed to both *create* a login account and to *authorize* the account creation.

Constrains may apply even on an information object instance level. For example could a User be restricted only to exercise his permissions only on information objects he is the registered owner of, or has been delegated access to.

Claims-based Identity[2] is a common way for applications to acquire Identity Attributes for Actors inside own organization and in other organizations. Claims-based identity

[1] https://en.wikipedia.org/wiki/Role-based_access_control
[2] https://en.wikipedia.org/wiki/Claims-based_identity

abstracts the individual elements of identity and access control into two parts: a notion of claims, and the concept of an issuer or an authority.

A claim is a statement about what an Actor *is,* i.e. certain Attributes, which could include information used for Access Control, such as Organizational belonging and/or authorized Roles. Claims are packaged into one or more TOKENS that are then issued by an issuer (provider), commonly known as a Security Token Service (STS).

Permissions are specific to the Service, an Actor wishes to interact with. Service specific Roles may be defined *by the Service,* as a group of Permissions and/or Constraints. Roles are however more frequently defined *by users organization* to define the duties or responsibilities of Users. These Roles may be in this case, a translation between Roles defined by the organization external to the Service, and the group of Permissions or Constraints, could be registered with the Service, and allow the user organization to manage permissions of their own users, using own Roles, if the organizational Roles are registered with the Security Token Service, are transferred to the Service with the Claims (Tokens) as part of the Authentication process.

Claims-based Identity has the potential to simplify authentication logic for individual services, because those services do not have to provide mechanisms for account creation, validation of Attributes, password creation, reset, and so on. Furthermore, claims-based identity enables applications to know certain facts about the Identity (the Attributes – such as Roles defined by the User's company), without having to interrogate the user to determine those facts. The facts, or claims, are transported in an "envelope" called a secure token. Claims-based identity can greatly simplify the authentication process because the user does not have to sign in multiple times to multiple applications.

6.2 Information Object Identities

Unique IDs may also be needed to identify information objects that describe specific transactions. Transactional information objects (sometimes called Events) do not perform actions by themselves – they represent a managed collection of data or information, related to a certain transaction, process or event, only accessible to those Actors with relevant Permissions.

In SeaSWIM, the need for managing information objects shared between a large number of stakeholders such as ship Voyages and Port Calls results in the need for globally unique references – i.e. unique identifiers.

6.3 Identifiers

Different Identities must be uniquely identifiable within their context of use. Identifiers (the Attribute that identifies an Identity) must thus be unique. In order to achieve interoperability, Identifiers used in SeaSWIM must be based on standards that ensure uniqueness, and enable Actors from different domains to interact.

Different types of identifiers for Actors are common in certain domains, for instance IMO numbers to identify ships, country and company registration numbers to identify Companies, etc.

Transactional information objects such as Voyages and Port Calls may be accessible by many different Actors, operating in different contexts, and thus, their identifiers must also be based on standards that ensure uniqueness.

6.4 Services and interactions

SeaSWIM is a Service Oriented Architecture, where Actors may interact with the functions of (Data) Services through Service Interfaces, depending on Actors authorizations – i.e. which Roles the Actor has been authorized, and which Permissions those Roles translate to.

Users (Actors with a social core) will access Services using some kind of HMI application, System Actors (Servers, other Services) will access a Service through Interfaces.

6.4.1 Services – Description, composition and interfaces

A Service - as you can see in Fig. 1 - may be

- An *Atomic* service (i.e. completely self-contained)
- A *Composed* service (Composed of several services)

A tree structure may be used to describe which composed services are using an Atomic service, or which atomic (or composed) services are part of a Composed Service.

In a Composed Service, one Service may be considered as an Actor of another Service.

A complete design of a Service may need to consider issues and standards related to

- Business / Regulatory matters incl. security required user competences, etc
- Data / Information
- Functions (incl. Permissions, Constraints)
- Communication
- Physical components and connections

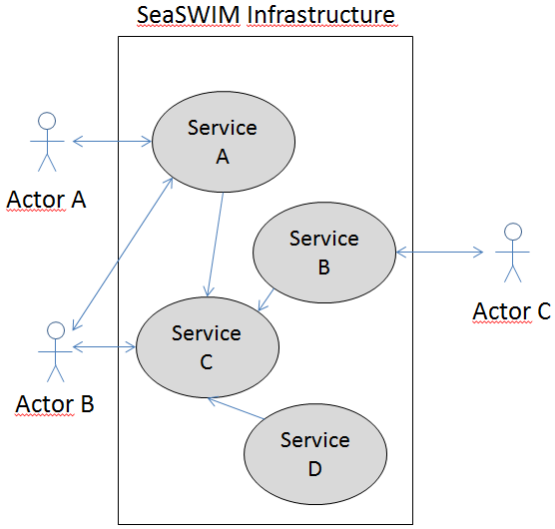


Figure 3: SeaSWIM infrastructure

The focus of the Use Cases in this Requirement analysis relates to Actors interaction with (external) interfaces of a Service and will primarily focus on:

1. The *Information/Data* that can be exchanged with or manipulated by a Service
2. The *Functions* accessible by Actors (specified input, output, required sequence of interactions)
3. Which *Permissions* or *Constraints* (if any) that are needed to regulate Actors access to *Functions (*and recommended Roles that group relevant Permissions or Constraints)

Any Service which handles Functions or Data that require Access Control, will need to include a Logon Function which can assess an Actors credentials and determine which authorized Roles translate into which Permissions and/or Constraints, before the Actor is allowed to access other Functions.

In an Atomic service (Service F in the Figure below), this may be a Service specific login function. In this case, Service F must also provide Functions for authorizing the Roles and Permissions of Actors.

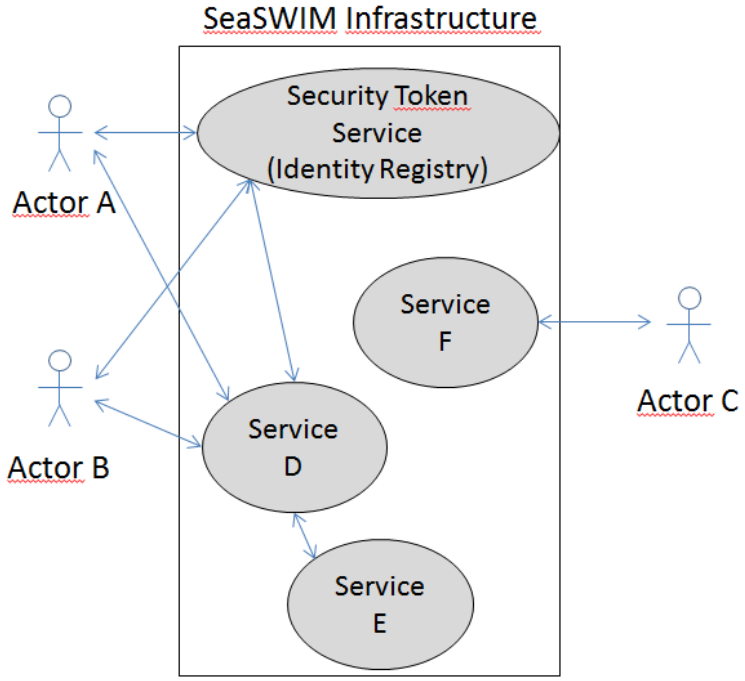


Figure 4: Use of a Security Token Service

Using a trusted Security Token Service, Service D will not need to manage Actor Identities and validate their (global) Attributes, nor implement login functions.

Service D will however need to register which Actors or which Roles authorized by whom - are permitted to access the Service and translate into which Service specific Permissions.

This will allow Actors 'Single Sign On' to multiple or composed services, and may allow organizations external to the provider of the Service to manage (authorize) Roles for other Actors (e.g. a company managing Roles for their own employees) without the need for Service D to implement Role management functions.

A first proposal for a taxonomy is shown in the following table:

Table 2: proposed taxonomy

Service Identification
- Service ID
- Service Name (max 50 characters)
- Service Description (max 300 characters)
- Service Context (under which circumstances this service is consumed (when, where etc.)?)
- Nature of the service (informational (data), application)
- Service type (transactional, analytical, transformational)
- Mandated or optional
- Service Status
  ○ proposed / under review / release / retired
	Service Composition and Interfaces
	- Service Composition (documented as a service tree)
	  ○ Atomic service (what composed services are using it)
	  ○ Composed service (what atomic services are part of it)
	
	- Service Interfaces
	  ○ input
	  ○ output
	  ○ ID requirements (details of authentication/authorization of service consumer)

Service Channel and Engagement Management - ID requirements to access service - Open access or selected users - Channels provided to access service - Access level	**Service Relationships** - Requirements (what requirement(s) are addressed by this service?) - Standards (what standards are related to this service?) - Other services (predecessor, successor, previous version)

Service Interaction Patterns
- Details on the interaction pattern, e.g.
  ○ service is called by consumer
  ○ service is offered to consumer
  ○ service request needs to be confirmed
  ○ number of parties involved
  ○ etc
	Service Governance, Risk and Quality Management
	- Service Owner (incl. contractual arrangements)
	- Exclusivity arrangements (i.e., one single provider?)
	- Service Level Agreements (e.g., availability, responsiveness, quality)
	- Service Contracts (i.e. ad-hoc or contract required?)
	- Service charging model (e.g, per consumption, per time period, etc.)
	- Service risk profile and mitigation
	- Service Review (frequency, type of review)

	- Service assessment (channels for service feedback)

1) Service Identification

This group of attributes captures attributes needed to clearly identify each service via a unique Service ID. This ID is needed to address services. Further attributes allow characterising the service and in particular to specify the context in which this service is required. Examples for such contexts could be time-based (e.g., hours to arrival), location-based or message-based (e.g., pilot has been allocated). If a service is mandated, defined events could call and execute the service automatically. Optional services will require different communication services making sure possible consumers are aware of these services. Each service is classified as being either transactional (e.g., conduct route planning), analytical (e.g., consolidate and visualise routes) or transformational (e.g., innovation services dedicated to exploring new services).

The service status, and its change, is an essential attribute for the overall governance for the service.

2) Service Channel and Engagement

This group of attributes captures a 'black-box' view on the service, i.e. how to interact with the service including requirements for identification (open or identification required). Each service will be related to certain communication channels describing how the service can be accessed and how the service is delivered. A service might have different access levels depending on the access rights and requirements of the service consumer.

3) Service Interaction Patterns

Depending on the sequence of interactions between the provider and the consumer, different patterns can be differentiated. Each service is linked to one or more of these patterns defining the sequence of interactions. Examples might be if a service requested, if a service is offered based on states of an identified actor, if a confirmation is needed after a request or if the interaction is bi-directional or multi-directional, i.e. involving more than one stakeholder. A detailed list of relevant interaction patterns will be made available.

4) Service Composition and Interfaces

Services can be differentiated into atomic services (e.g., weather forecast) and composed services (e.g., weather-based route optimisation). For each atomic service, relationships to composed services need to be maintained while each composed service needs to be broken down into atomic services in the form of a service tree. This information allows hierarchical navigation within the service ecosystem and tracing implication in case of a service failure.

Service interfaces describe the (mandated or optional) information and their format needed to interact with the service and are differentiated along the service lifecycle (e.g., request vs confirmation). They also capture identification requirements for each interface. For example, simple enquiries (e.g., availability check) might not require any identification whereas reservations will require it.

5) Service Relationships

In addition to the hierarchical relationships between services as captured in (4), services have further relationships with other entities. They have various relationships with other services capturing service value chains in the form of predecessor-successor relationship. A service could also replace another service (version management or complete new service) or be an alternative for another service. Services can be linked to defined requirements to justify the existence of the service and to facilitate requirements monitoring. Finally, services could be linked to standards. This is relevant for external assessments and to identify services in need for updates in case new standards emerge.

6) Service Governance, Risk and Quality Management

Finally, an entire cluster of service attributes captures most of the compliance, governance and risk attributes. This includes ownership and related exclusivity arrangements. Service contracts and service level agreements provide formalised engagement and quality evaluation models. A dedicated service charging model captures the economic engagement and pricing model. The risk profile of the service (e.g., likelihood of failure, impact, and frequency of risk assessment) is captured here as well. Finally, formal service reviews and assessment link to the overall monitoring and quality assessment of the service.

38 partners from 13 countries -
Creating a safer more efficient and environmentally friendly maritime sector

Demonstrating the function and business value of the Sea Traffic Management concept and its services.

SAFETY - ENVIRONMENT - EFFICIENCY

Swedish Maritime Administration ◦ SSPA ◦ RISE Viktoria ◦ Transas/ Wärtsilä Voyage ◦ Chalmers University of Technology ◦ The Swedish Meteorological and Hydrological Institute ◦ Danish Maritime Authority ◦ Navicon ◦ Novia University of Applied Sciences ◦ Fraunhofer ◦ Carnival Corp. ◦ Italian Ministry of Transport ◦ SASEMAR ◦ Valencia Port Authority ◦ Valencia Port Foundation ◦ CIMNE ◦ University of Catalonia ◦ Norwegian Coastal Administration ◦ GS1 ◦ Cyprus University of Technology ◦ Port of Barcelona ◦ Costa Crociere ◦ Svitzer ◦ OFFIS ◦ Finnish Transport Agency ◦ Southampton Solent University ◦ Frequentis ◦ Wärtsilä SAM Electronics ◦ University of Flensburg ◦ Airbus ◦ Maritiem Instituut Willem Barentsz ◦ SAAB TransponderTech AB ◦ University of Oldenburg ◦ Magellan ◦ Furuno Finland ◦ Rörvik ◦ University of Southampton ◦ HiQ

www.stmvalidation.eu

Co-financed by the Connecting Europe Facility of the European Union