C80-10.5.4

IALA Technical Service:

Service Design for VTS Traffic Clearance Service using SECOM

Version 1.0

June 2024

Contents

1 Introduction

This document was produced as part of the work of IALA joint VTS-ENAV task group on development of technical service specifications for VTS. The document is structured according to the IALA Guideline *G1128 The Specification of e-Navigation Technical Services* [1].

1.1 Purpose of the Document

The purpose of this service design is to provide a design for the implementation of the digital service of VTS Traffic Clearance Service using SECOM and S-212 as the S-100 series data model for the actual message payload.

The aim is to document the key aspects of the VTS Traffic Clearance Service using SECOM service so that implementers know how the specification is to be implemented in an interoperable way and how the interaction between the actors defined in the specification is implemented using the APIs defined in SECOM. For this purpose, we define:

- Why SECOM was chosen to facilitate the implementation.
- The main elements of the service:
  - the components it is composed of,
  - interfaces provided,
  - the operations of the service,
  - and the parameters in the operations.
- The data model of the service
- The dynamic behaviour of the service, i.e. how the use cases defined in the specification are actually technically implemented.

1.2 Intended Readership

This service specification is intended to be read by service architects, system engineers and developers in charge of designing and developing an instance of the VTS Traffic Clearance Service using SECOM.

Furthermore, this service specification is intended to be read by enterprise architects, service architects, information architects, system engineers and developers in pursuing architecting, designing and development activities of other related services.

1.3 Inputs from Other Sources

Reading this design document requires a thorough understanding of the related Service Specification.

As this design uses SECOM and an understanding of IEC 63173-2 SECOM is recommended.

This design is based on Service Design – Template SECOM REST and uses text from the template where valid.

2 Service Identification

The purpose of this chapter is to provide a unique identification of the service and describe where the service is in terms of the engineering lifecycle.

Name	*VTS Traffic Clearance Service Technical Design using SECOM*
Implements	Service Specification for VTS Traffic Clearance 1.2 urn:mrn:iala:techsvc:ss:vts:tcs:1.2
ID	*urn:mrn:iala:techsvc:sd:vts:tcs:secom:0.3*
Version	*0.3*
Description	*The VTS Traffic Clearance Service Design using SECOM specifies how the VTS Traffic Clearance specification is to be implemented using SECOM to facilitate the communication between ship and shore systems.*
Keywords	*VTS, MS1, Traffic Clearance, Ship Traffic Management, S-212, S-421, SECOM*
Architect(s)	*Ramin Miraftabi*
Status	*Provisional*

3 Technology Introduction

3.1 General

This design realizes the service specification [6] using SECOM as defined in **Erreur ! Source du renvoi introuvable.**.

The services conforming to this design must be implemented with REST APIs using HTTPS with TLS protection to encrypt all communication in transit.

3.2 Service Technology and transportation protocol

Reference: IEC 63173-2 SECOM v1.0.0 Clause 5.3 Service Technology

The technology (architectural style) chosen is REST (REpresentational State Transfer) upon HTTP/1.1 (RFC 7231).

3.3 Security

3.3.1 Communication channel security

Reference: IEC 63173-2 SECOM v1.0.0 Clause 6 SECOM communication channel security

The channel security between the service and a consumer are:

- HTTP/1.1 according to RFC-7231
- HTTPS over TLS according to RFC-2818

Valid versions of TLS for this version of service design template are:

- TLS version 1.2 (RFC-5246)
- TLS version 1.3 (RFC-8446)

X.509 Certificates are used in the TLS according to RFC 5280 and RFC 2459.

Certificates shall be verified with OCSP and/or CRL methods.

3.3.2 Data Protection

Reference: IEC 63173-2 SECOM v1.0.0 Clause 7 SECOM data protection

Reference: IHO Standard S-100 ed5.0.0 Part 15 Data Protection Scheme

The data is mandatory to be signed by the sender to enable data authentication and integrity check by the receiver.

The data can optionally be encrypted by the sender, and the sender is responsible for exchanging the encryption key to receiver.

The data (one or more data files) can optionally be packaged and compressed before signed.

3.3.3 Data Signature

Reference: IEC 63173-2 SECOM v1.0.0 Clause 7.3 Data authentication and signing

Reference: IHO Standard S-100 ed5.2.0 Part 15-8 Data Authentication

Reference: NIST Digital Signature Standard (DSS–FIPS Publication 186)

The algorithm for signing data is ECDSA-384 and SHA256.

The signature is transported in HEX.

3.3.4 Data Encryption

Reference: IEC 63173-2 SECOM v1.0.0 Clause 7.4 Data encryption

Reference: IHO Standard S-100 ed5.0.0 Part 15-6 Data Encryption

The encryption algorithm for encryption is AES (128, 192 or 256 bit) and CBC mode.

The symmetric encryption key can be exchanged by different means, including using the SECOM REST API and Diffie Helman to encrypt and exchange the encryption key.

4 Service Design Overview

4.1 General

The design uses SECOM defined APIs. As such, it is important to understand that both the traffic clearance service and its consumers must be able to function as client and server as understood in the traditional HTTP world. As such from here on when the term service is used, it applies to the traffic clearance service and the consumer is the ship, agent, etc that is requesting traffic clearance from VTS.

This design does not concern itself with how the service will communicate with the VTS system. The instances of this design may be developed as components directly integrated with the VTS system or as independent microservices that communicate with the VTS system via different integration mechanisms e.g., APIs or by emitting and consuming events.

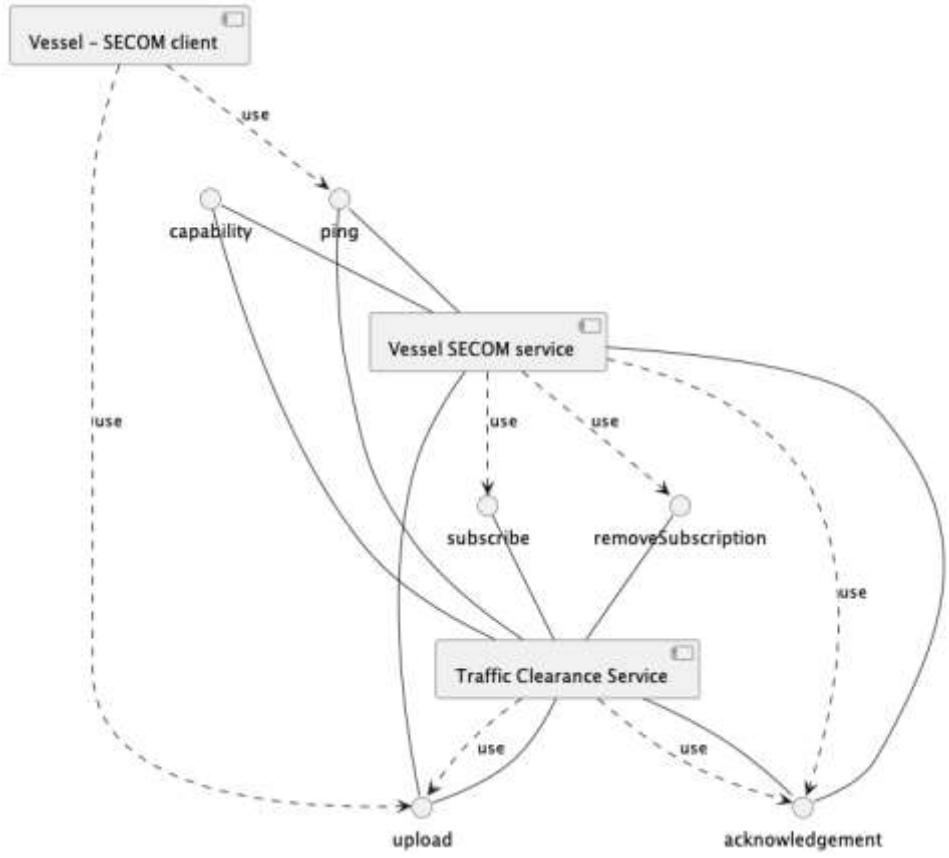
4.2 Service interfaces

SECOM does not require that all the interfaces defined in the standard must be implemented. Thus, for the purposes of this service and its consumers, only the following interfaces are required:

Interface	SECOM Reference	Comment
Capability	IEC 63173-2 SECOM v1.0.0 Clause 5.7.13 service interface – Capability	This interface is called when client asks for the service capabilities. Required by SECOM standard.
Ping	IEC 63173-2 SECOM v1.0.0 Clause 5.7.14 service interface – Ping	This interface is called when client checks the availability of the service. Required by SECOM standard.
Upload	IEC 63173-2 SECOM v1.0.0 Clause 5.7.2 service interface – Upload	This interface is called when client uploads (pushes) data to the service. The sender (client) decides format and protection of the data.
Acknowledgement	IEC 63173-2 SECOM v1.0.0 Clause 5.7.4 service interface – Acknowledgement	This interface is called when client or server initiates subscription on data from the service. Response is given with interface Upload

		and Subscription Notification.
Subscription	IEC 63173-2 SECOM v1.0.0 Clause 5.7.10 service interface – Subscription	This interface is called when client creates a subscription.
Remove Subscription	IEC 63173-2 SECOM v1.0.0 Clause 5.7.11 service interface – Remove Subscription	This interface is called when client removes subscription.

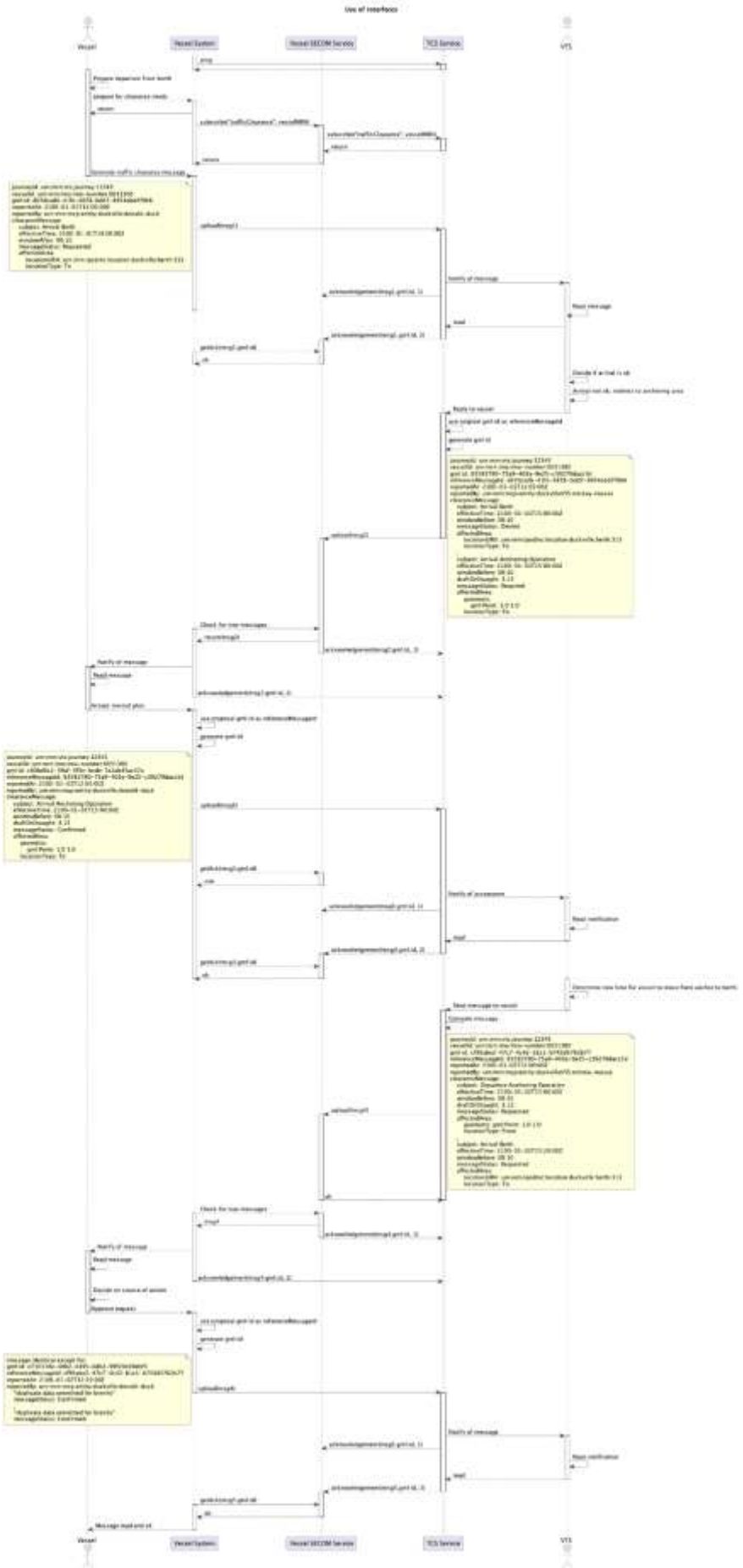
The service does not require encryption and as such, no interfaces for the exchange of keys is required and is out of scope for the service.



The following diagram illustrates the most extreme use case of the communication between the service and client and illustrates the need for all the interfaces. This example assumes that service endpoint is already known through prior configuration or service discovery from a service registry. Note, the data is not XML in this example and parameters only contain the payload required to describe the business logic.

Note that the communication described between vessel system and vessel SECOM service is nonnormative.

All unused interfaces of SECOM should be implemented to return HTTP 501 as specified in [7].


Use of interfaces
Vessel
Vessel System
Vessel SECOM Service
TCS Service
VTS

We will examine the diagram in more detail in 7.

There are three components that are of interest from the perspective of the service design:

- The service has a SECOM-component which supports the SECOM REST APIs defined in the table above. All other components of the service are left to the decisions of the implementing party.
- The vessel has a SECOM-component which will accepts the incoming connections from the service and store all messages until delivered to the vessel. This interface is typically on a shoreside server as it must be always available and at a static address.
- The vessel has an implementation of a SECOM client which allows it to make direct SECOM calls to the service without having to proxy all calls via the SECOM-component on shore.

In this service design we will not define the communication between the service and VTS system or the vessel and the vessel's shoreside SECOM interface. These are specific for each implementation and depend on the VTS system and vessel's system.

4.3 Service Discovery

Services implemented according to this design must submit their instance description to a valid service registry that follows the Maritime Service Registry definition [11].

An XML template for the instance description is provided as an annex to this design. Appendix A.

5 Physical Data Model

The data model of the service is a combination of JSON (SECOM calls) and XML (the S-212 payload). The SECOM JSON is defined in [7] section 5.

The S-212 data that is used by the service is a subset of S-212. The following elements, attributes and enumeration values must be supported by the service and its clients.

XXX TODO once S-212 is discussed and relatively stable XXX

6 Service Interface Behaviour

As defined by SECOM, all communication between the components of the service that are in the scope of this design document is done via REST calls.

Additional information on the interfaces and parameters is available in the attached OpenAPI template of service in Appendix B.

6.1 Applicable SECOM Interfaces

The Capability and Ping interfaces are not discussed in this design as they follow the requirements defined in IEC 63173-2 SECOM and need no further elaboration here.

All interface descriptions below only have the information necessary for the business logic of this service. All definitions and descriptions that are directly derived from the SECOM standard left to be read from the SECOM standard and the API documentation template in TODO create Annex.

All SECOM communication is done via REST APIs with JSON as the data format for the SECOM data and XML for the S-212 data.

For all interface requests the following definitions of the content of fields apply:

- transactionIdentifier – must be the same as the gml:id of the VTSDigitalInformationMessage element in the data being passed.

6.1.1 Upload

The Upload interface must be available both on the service as well as the SECOM interface of the vessel. The URL of the upload interface for the SECOM interface of the vessel must be passed in the callbackUrl parameter given when subscribing to traffic clearance messages from VTS.

The EnvelopeUploadObject according to IEC 63173-2 SECOM fields that influence this service are:

- containerType – must always be “NONE”
- dataProductType – must always be “S212”
- exchangeMetadata
    - dataProtection – must always be 0 (unencrypted)
    - protectionScheme – must always be “SECOM”
    - compressionFlag – must always be 0 (uncompressed)

- fromSubscription – must always be true when sent from service to vessel as service never broadcasts without subscription; must always be false when sent from vessel to service as service does not need to subscribe to traffic clearance messages.
- ackRequest – TODO define what ACK we are interested in: delivered, opened or both
- data – S-212 VTSDigitalInformationMessage with 1-2 ClearanceMessage's in the content. Incoming data with no ClearanceMessage's must return a value 0 in SECOM_ResponseCode to signify missing required data for service.

The return value of the upload interface must follow the SECOM standard. The message is not expected and should only be returned in the case of an error to provide additional information is available.

6.1.2 Acknowledgement

There are no specific business rules that must be defined here for the acknowledgment interface that are not covered by the SECOM API specification document.

The requested level of acknowledgment by the service or the consumer must always be: 3 – delivered and opened acknowledgment requested.

6.1.3 Subscription

The subscription interface must be implemented in the traffic clearance service. It is not needed in the consumer and thus should not be implemented.

The following parameters of the SubscriptionRequestObject are expected to be passed as a part of the request from the consumer:

- containerType – must be "NONE"
- dataProductType – must always be "S212"
- dataReference – UUID that is equal to the gml:id of the VTSDigitalInformationMessage in the payload.
- productVersion – is not expected but may be any valid version of S-212.
- geometry – should not be passed, there is no requirement that the service supports geometry-based subscriptions.
- unlocode – should not be passed, there is no requirement that the service supports unlocode-based subscriptions
- subscriptionPeriodStart – may be passed, if not passed service will default to time of reception of call to interface

- subscriptionPeriodEnd – may be passed but not required. Due to uncertainty of departure from VTS area consumers should always terminate the subscription by calling the remove subscription interface when departing VTS area.
- callbackUrl – The endpoint of the consumer's SECOM service that accepts the upload and acknowledgment interface calls. The endpoint must be defined in a way that appending the SECOM standard /v1/subscription and /v1/acknowledgement produces a valid URL. If the callbackUrl is not a part of the subscription, the traffic clearance service must search for the vessel's SECOM service from a service registry.

Note that callbackUrl is not a part of the current SECOM standard but has been submitted as a recommended change to reduce the need for registration of SECOM consumers in service registries.

The returned SubscriptionResponseObject contains the following:

- message – optional. Consumers may or may not support this.
- subscriptionIdentifier – must have an UUID that can be used to remove the subscription once the vessel departs VTS area.

The service must use the MRN of the vessel retrieved from the certificate submitted in the request headers or TLS transport to identify the vessel for which the subscription is created. The vessel must not receive messages intended for other vessels as a result of this subscription.

6.1.4 Remove Subscription

The remove subscription interface must be implemented in the traffic clearance service. It is not needed in the consumer and thus should not be implemented.

The removeSubscriptionObject must have the subscriptionIdentifier returned when the subscription was created.

The consumer should call removeSubscription when departing the VTS area to clear unnecessary subscriptions.

6.2 Signatures and certificates

All the envelope signatures and certificates used must be signed by the VTS the Traffic Clearance Service is operating under or the consumer (vessel) that it is serving. The data is not signed separately.

The signatures must be issued by a Maritime Identity Registry as specified in [10].

The service must have a method of automatically obtaining new keys and rotating them as specified in [10].

7 Service Dynamic Behaviour

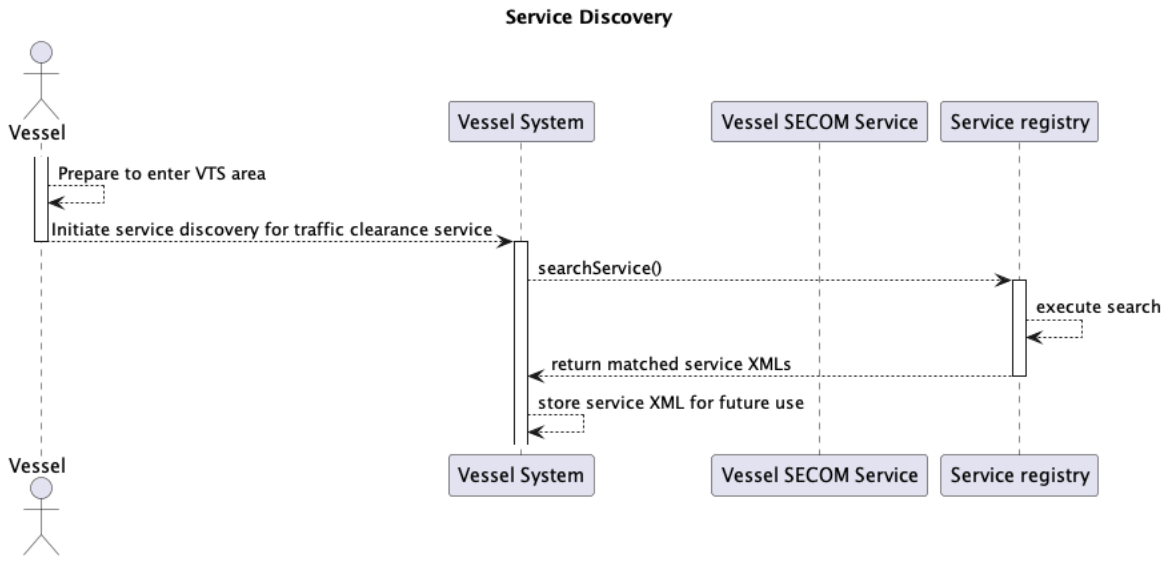
In the following diagrams and descriptions, the communication between the vessel's onboard systems and its SECOM service is out of scope for the purposes of this design.

Similarly, the communication and interfaces between the traffic clearance service and the VTS system is out of scope of this design.

7.1 Service discovery

To find a suitable VTS service the vessel will search for a traffic clearance service that implements this design from a service registry, for example one developed according to the Maritime Service Registry (MSR) specification from [11].

The search can be done by supplying a route and design document MRN as parameters and will return the information storing in MSR for the instances along the route that implement this design. The returned information follows the implementation metadata XML as defined in G1128.



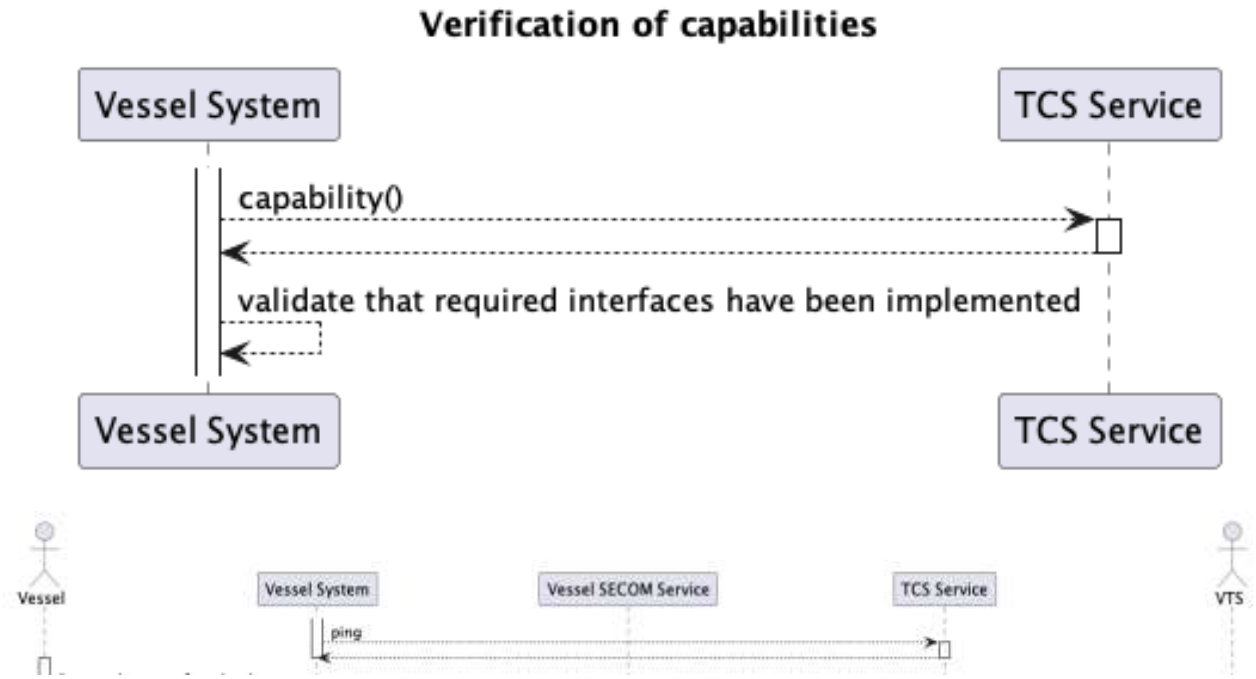
7.2 Checking capabilities

A standard SECOM approach would encourage a check of service capabilities by the vessel by calling the capability interface of the service. Since this design does not allow for any optional interfaces to be implemented and all functionalities must be implemented by a conforming implementation this step can be skipped.

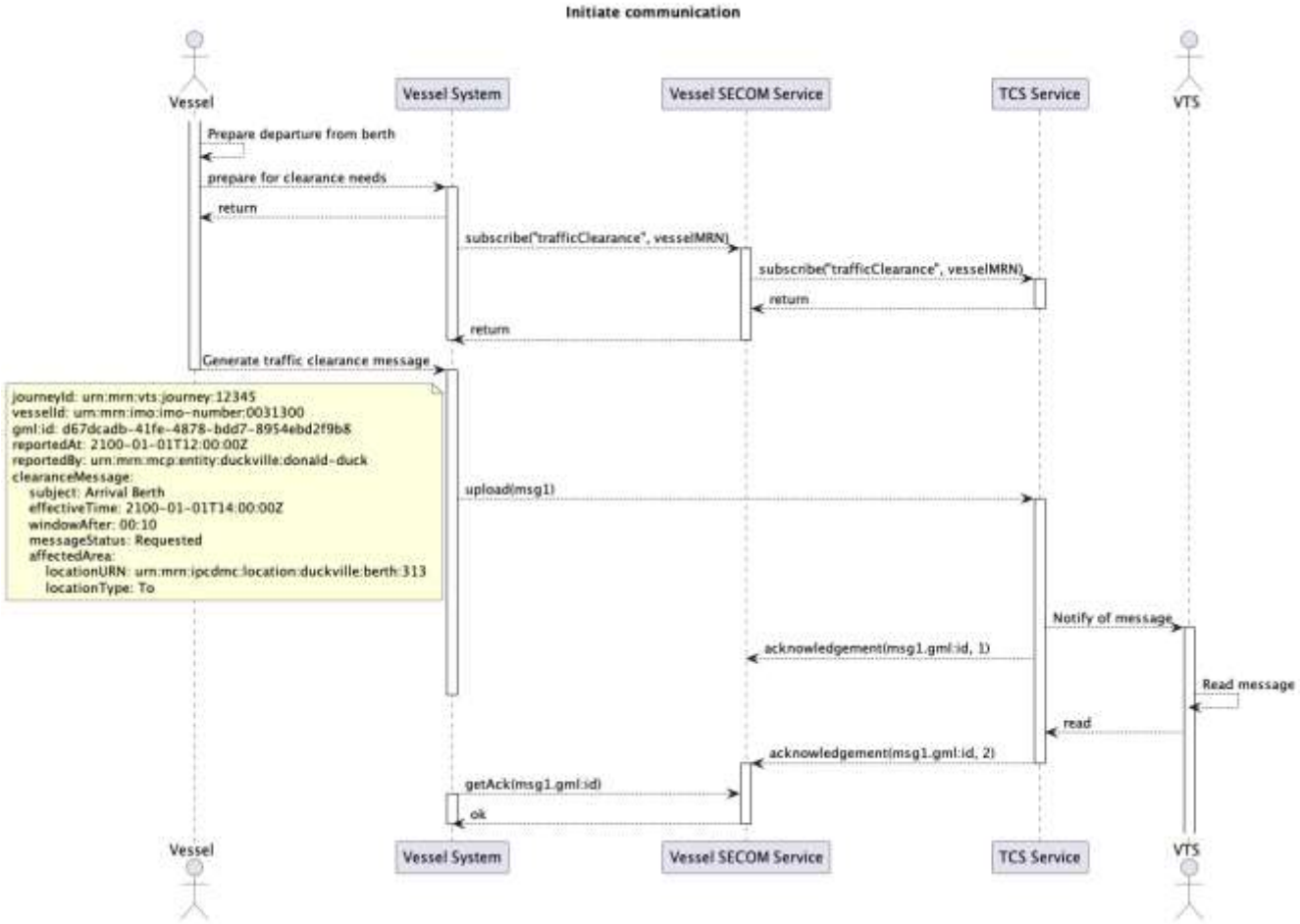
However, since a capability check is not required, it is recommended that the ping interface is called before submitting a traffic clearance request to ensure that the server is still available

at the endpoint returned during service discovery. If the ping is not successful, then service discovery must be redone to ensure that the service endpoint has not been changed.

If the service endpoint has not been changed in the service registry, then it must be assumed that the service is down, and the vessel must choose to retry in a suitable interval or resort to voice communication for traffic clearance.



7.3 Sending the initial traffic clearance message from vessel to VTS



As seen in the diagram, the first step is to use the upload interface of the service to send the initial traffic clearance message to VTS. Once the traffic clearance service has forwarded the message to the VTS system and gets confirmation that the message has been opened and SECOM acknowledgment must be sent. For this to work, the vessel must have subscribed to traffic clearance messages for the vessel so that the service has an endpoint to which to send the acknowledgment message.

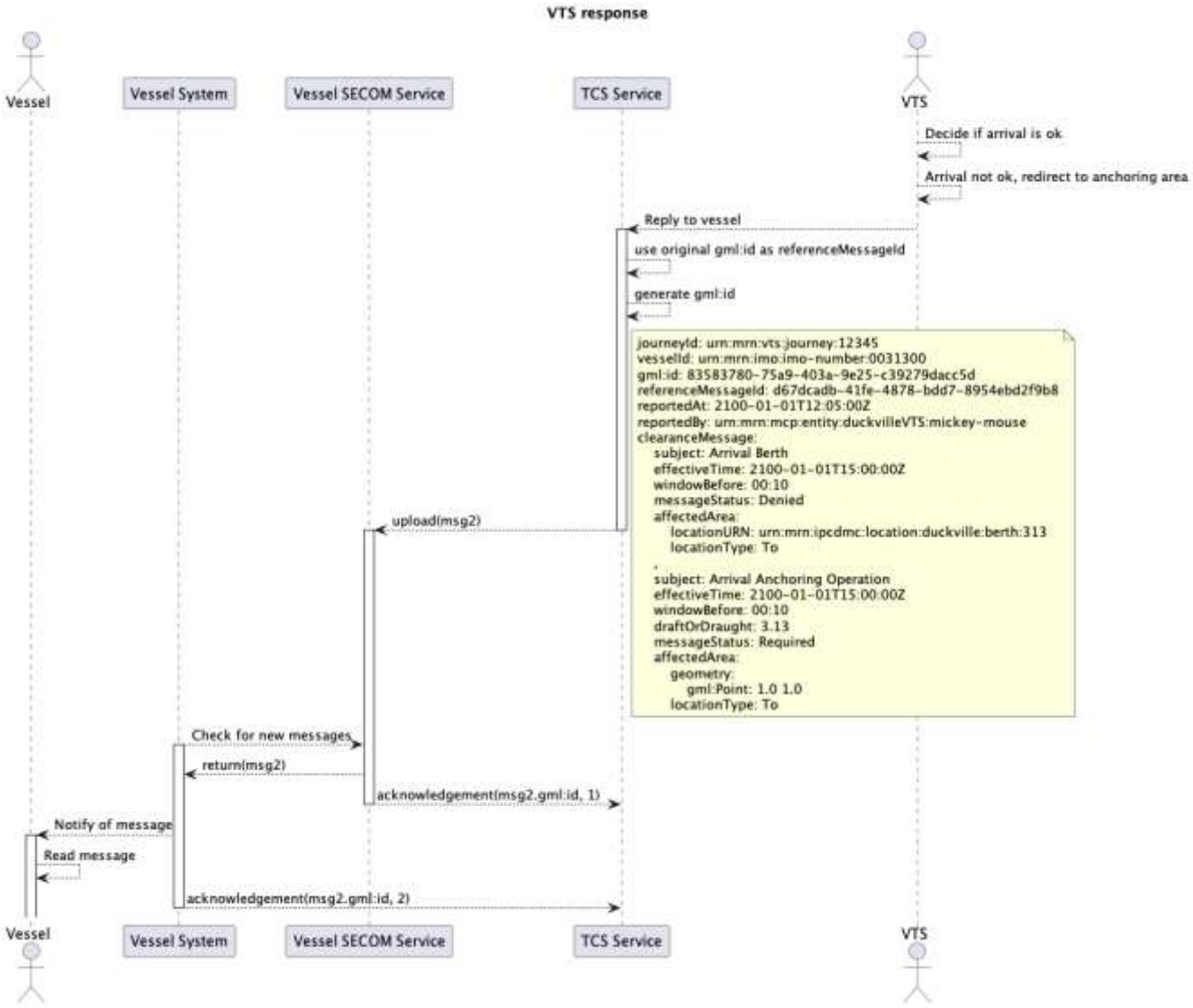
The acknowledgment message is received by the vessel's SECOM service which needs to deliver the acknowledgment to the vessel systems.

7.4 Responses to the clearance message from VTS

The acknowledgment described in the previous section is a technical acknowledgment that the message has been delivered or read but does not constitute an actual response. The response, no matter if it is a request to change the requested time or type of clearance must be sent in a separate call to the upload interface of the vessel's SECOM service to which the endpoint has been given as a parameter to the call to the traffic clearance service's subscription interface.

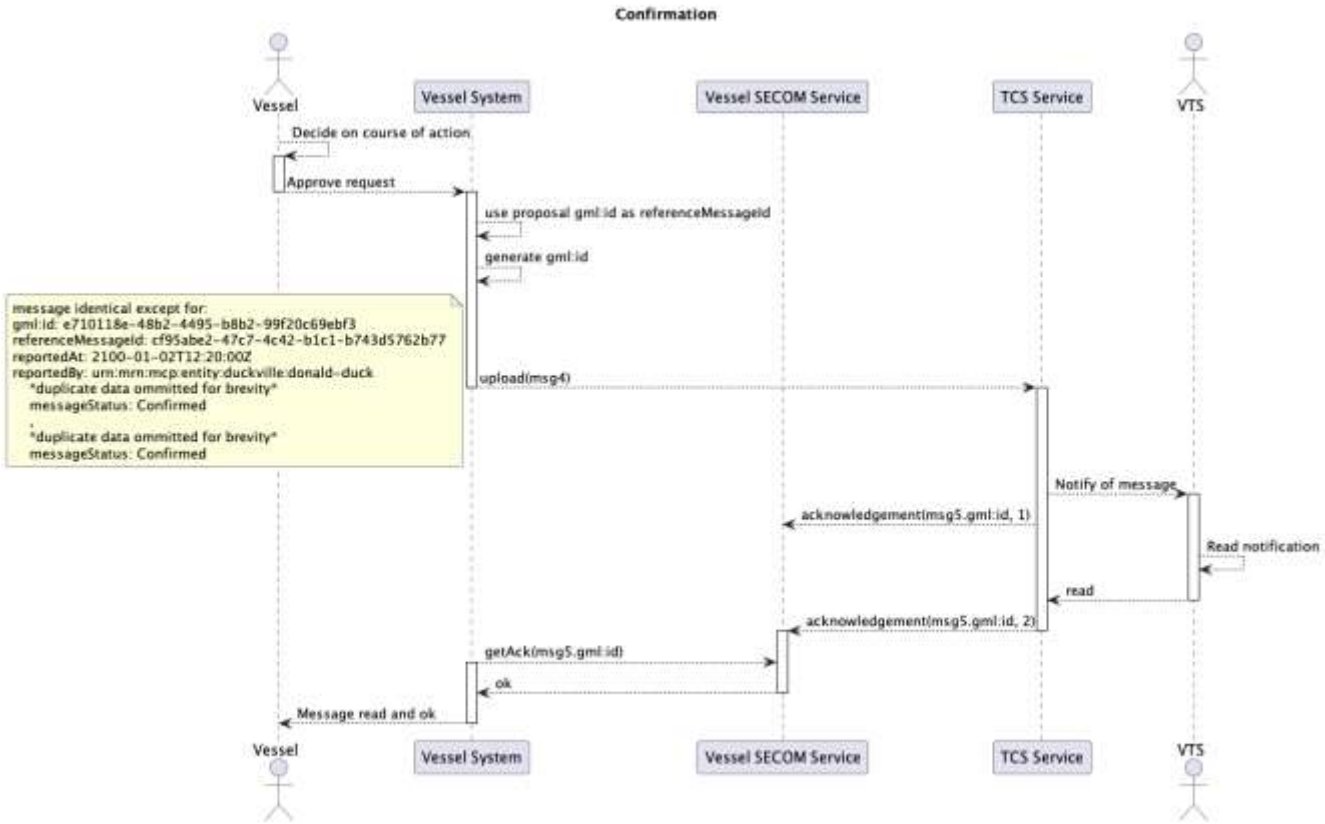
The message from VTS must have the referenceMessageId field filled with the gml:id of the initial message from the vessel as the value. The gml:id of the message from VTS to the vessel must be a new id.

The messageStatus of the clearance message is set as needed.



As is the case in the initial upload an acknowledgement must be requested once the message from VTS has been read on the vessel. Not just when it has been technically delivered.

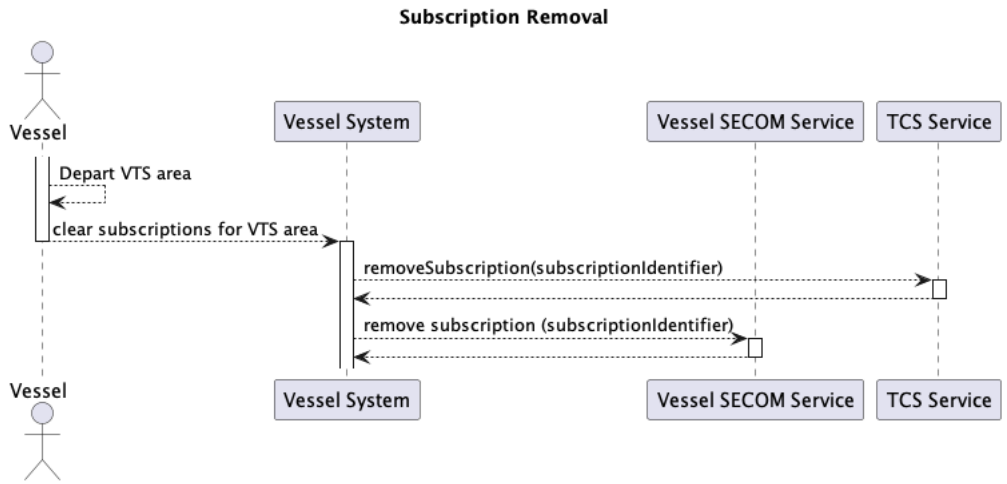
If more communication is needed between the vessel and VTS the same pattern of using the previous messages gml:id as the referenceMessageId of the response must be followed.



If the messageStatus of the received message is one that does not require an action (i.e. Confirmed, Denied, Cancelled) a response is no longer needed and the read acknowledgment is sufficient to signal that the message has been read and accepted. It is important to note that if the message was sent with a messageStatus of Denied, unless the vessel changes route a new clearance should be requested.

7.5 Actions upon completion of the vessel's stay in the VTS's area

The title for this section intentionally does not refer to a journey of a vessel as a vessel may make multiple journeys in the area of a VTS and thus may not need to immediately take the actions requested in this section.



Once the vessel is leaving the area of the VTS the subscription to traffic clearance messages should be removed by calling the removeSubscription interface of the traffic clearance service.

This design intentionally does not require that the subscription be removed as there may be cases where the vessel frequents the VTS area and may need any traffic clearance messages that reflect changes in situation (see next section). It is recommended that the consumer of traffic clearance message be developed in a way that the time outside of a VTS area requiring a removal of subscription be is configurable to reflect the needs onboard.

7.6 Traffic clearance initiated by VTS

The specification describes an exceptional use case in which VTS needs to require changes to already submitted traffic clearances or to notify any incoming vessels that have current subscriptions to traffic clearance messages but no active clearances (see use case 6 in specification).

In this case, a generic clearance message may be sent to all of subscribers of traffic clearance messages or to a subset as selected by VTS operators. The messages will be sent to the vessels' SECOM service endpoints as defined in the subscriptions.

The messageStatus of the message in this case must be Required.

In this case if a change to an existing traffic clearance, the gml:id of the clearance message in which the approval was sent must be set to the referenceMessageId of the message being sent. If no existing clearance needs to be changed the referenceMessageId must not be sent.

8 References

Nr.		Reference
[1] IALA Guideline G1128		THE SPECIFICATION OF E-NAVIGATION TECHNICAL SERVICES
[2] IMO FAL.5 /Circ.52		Guidelines for Harmonized Communication and Electronic Exchange of Operational Data for Port Calls
[3] IALA Recommendation R1023		MARITIME RESOURCE NAMES
[4] IHO Standard S-100	5.2.0	IHO Universal Hydrographic Data Model https://registry.iho.int/productspec/view.do?idx=197&product_ID=S-100
[5] IALA data model S-212		IALA VTS Digital Information Service Product Specification
[6] Service Specification for VTS Traffic Clearance	1.0	IALA VTS Digital Service Specification
[7] IEC 63173-2 SECOM	1.0.0	
[8] Service Design – Template SECOM REST		G1128 based template for service designs using SECOM REST
[9] NIST Digital Signature Standard (DSS–FIPS Publication 186)		
[10] Future IALA Guideline on Maritime Identity Registry	*TBD*	IALA guideline based on work in MCP. In process in DTEC.
[11] Future IALA Guideline on Maritime Service Regsitry	*TBD*	IALA guideline based on work in MCP. In process in DTEC.

9 Acronyms and Terminology

1.4 Acronyms

Term	Definition
API	Application Programming Interface
MRN	Maritime Resource Name
RTA/RTD	Requested time of arrival/departure
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier v4
XML	Extendible Mark-up Language
XSD	XML Schema Definition

1.5 Terminology

Term	Definition
Operational Node	A logical entity that performs activities. Note: nodes are specified independently of any physical realisation. Examples of operational nodes in the maritime context are: Maritime Control Center, Maritime Authority, Ship, Port, Weather Information Provider, …
Service	The provision of something (a non-physical object), by one, for the use of one or more others, regulated by formal definitions and mutual agreements. Services involve interactions between providers and consumers, which may be performed in a digital form (data exchanges) or through voice communication or written processes and procedures.
Service Consumer	A service consumer uses service instances provided by service providers. All users within the maritime domain can be service customers, e.g., ships and their crew, authorities, VTS centres, organizations (e.g., meteorological), commercial service providers, etc.
Service Data Model	Formal description of one dedicated service at logical level. The service data model is part of the service specification. Is typically defined in UML and/or XSD. If an external data model exists (e.g., a standard data model), then the service data model shall refer to it: each data item of the service data model shall be mapped to a data item defined in the external data model.
Service Interface	The communication mechanism of the service, i.e., interaction mechanism between service provider and service consumer. A service interface is characterised by a message exchange pattern and consists of service operations that are either allocated to the provider or the consumer of the service.
Service Operation	Functions or procedure which enables programmatic communication with a service via a service interface.
Service Physical Data Model	Describes the realisation of a dedicated service data model in a dedicated technology. This includes a detailed description of the data S-212 to be exchanged using the chosen technology. The actual format of the service physical data model depends on the chosen technology. Examples may be WSDL and XSD files (e.g., for SOAP services) or swagger (Open API) specifications

	(e.g., for REST services). If an external data model exists (e.g., a standard data model), then the service physical data model shall refer to it: each data item of the service physical data model shall be mapped to a data item defined in the external data model. In order to prove correct implementation of the service specification, there shall exist a mapping between the service physical data model and the service data model. This means, each data item used in the service physical data model shall be mapped to a corresponding data item of the service data model. (In case of existing mappings to a common external (standard) data model from both the service data model and the service physical data model, such a mapping is implicitly given.)
Service Provider	A service provider provides instances of services according to a service specification and service instance description. All users within the maritime domain can be service providers, e.g., authorities, VTS centres, organizations (e.g., meteorological), commercial service providers, etc.

Appendix A Service implementation XML template

TODO service implementation XML template

Appendix B Service instance OpenAPI definition template

TODO service instance template OpenAPI definition