Input paper: [1] VTS54-9.1.1

Input paper for the following Committee(s):	check as appropriate		Purpose of paper:
□ ARM	□ ENG	□ PAP	**X** Input
□ ENAV	**X** VTS		□ Information

Agenda item [2]	9.1
Technical Domain / Task Number [2]	2.5.2……
Author(s) / Submitter(s)	Agency for Maritime and Coastal Services, Belgium
	DLR, Germany
	Fintraffic, Finland
	Finnish Transport Infrastructure Agency, Finland
	Navelink
	AIVeNautics, Republic of Korea

VTS Technical Services - roadmap

1 SUMMARY

During VTS52 a ENAV/VTS taskgroup for tasks 2.3.1 *"Develop a Product Specification S-212 under the S-100 framework for VTS"* and 2.5.1 *"Development of technical service specifications for digital data exchange between VTS and other entities - primarily ships"* was established.

During VTS53 the joined taskgroup created a VTS Digital Services System Architecture description. This architecture description consists of the technical services as well as the S-100 product specifications.

An inter-sessional meeting was organized for the joined taskgroup and taskgroup 1.3.2 from WG1 *"Develop guidance on VTS Digital communications (operational aspects)"*. The taskgroup from WG1 provides the necessary operational use cases, so the taskgroups under WG2 can define the technical services and product specifications.

During the inter-sessional meeting two initial technical service (Traffic Clearance Service and route exchange) was presented and discussed. Following topics are to be looked at more closely:

- SECOM (IEC 63173-2)
- Maritime Connectivity Platform
- S-212
- Liaison to DTEC

1.1 SECOM (IEC 63173-2)

IMO has adopted the IEC standard 63173-2 for standardized communication infrastructure between shore and ships. It will be necessary to include this standard in the development of the technical services in order to

[1] Input document number, to be assigned by the Committee Secretary
[2] Leave open if uncertain

enable to exchange of information between shore and ship. SECOM requires both service discoverability and authentication.

For a better understanding of the architecture description it is recommended to include the SECOM standard.

1.2 S-421

The S-421 product specification contains a datamodel for ship routes - and is intended to be used in different route exchance services - including the route exchange service pertaining to the VTS domain.

1.3 Maritime Connectivity Platform (MCP)

To be able to cope with the issues of Service discovery and authentication, there is no viable alternative for the Maritime Conectivity Platform at this moment. For a better understanding of the architecture description it is recommended to include the MCP. More information at www.maritimeconnectivity.net.

1.4 S-212

To develop the first technical service S-211 (Port Call Messages) was referred to as almost all data-elements are available in this product specification. However, since S-211 is not developed or maintained by the VTS Committee it might not be the best option for the long term.

After the inter-sessional discussions have been continued with experts on S-100 and the VTS Committee chairs. The conclusion is that all VTS related data-elements from S-211 will be included in S-212, non VTS related data-elements will be excluded from S-212.

The data-model in S-212 is expected to be used in several technical services pertaining to the VTS area - including the initial 'traffic clearance' service.

1.5 Relation with the Open Digital Incubator initiative

The technical service specifications developed in TG2.5.1 “Development of technical service specifications for digital data exchange between VTS and other entities - primarily ships”, will be implemented and tested as part of the Open Digital Incubator initiative, and results from this will be reported to IALA once available.

1.6 Liaison to ENAV

It is recommended that a link is established between ENAV and VTS regarding the architecture for VTS Digital Services and the Common Shore-based System Architecture (CSSA). IALA Guidelines G1113 and G1114 describe the architecture for the Common Shore-based System Architecture.

The development of the VTS Digital Service architecture should stay aligned with the possible further development of the CSSA.

1.7 Relationship with taskgroup 1.3.2

Taskgroup 1.3.2 'Develop guidance on VTS Digital communications (operational aspects)' is submitting its own input to VTS54. This input inlcudes:

- Draft guideline on VTS Digital communication
  Which gives an overall operational description of how VTS's should operate when using the new technical services
- Specifications on route exchange
  The high level service specification (according to G1128) of a route exchange service for VTS. A draft technical design specification (following SECOM) is included in this document
- Common Operational picture
  A new technical service specification that is being developed (high level). TG 2.5.1 will be working on the technical parts of this as well.

1.8 Related documents (in annexes)

A. Working paper on the Architecture of the Digital Delivery of VTS Information

B. Work paper for VTS Traffic Clearance Service Specification (there has been some work on this after the inter-sessional meeting, primarily changing the utilised product specification from S-211 to S-212)

C. Draft technical design for route exchange service (there has also been some progress on this after the inter-sessional meeting). This is the technical design corresponding to the service specification for route exchange submitted by TG 1.3.2.

2 REFERENCES

[1] G1113 - DESIGN AND IMPLEMENTATION PRINCIPLES FOR HARMONIZED SYSTEM ARCHITECTURES OF SHORE-BASED INFRASTRUCTURE, version 1.1 (May 2015)

[2] G1114 - A TECHNICAL SPECIFICATION FOR THE COMMON SHORE-BASED SYSTEM ARCHITECTURE (CSSA), version 1.1 (May 2015)

[3] S-211 PRODUCT SPECIFICATION, Draft 1.0.0 (March 2019)

3 ACTION REQUESTED OF THE COMMITTEE

The Committee is requested to: (Body text)

1 Take notice of the fact that SECOM and MCP will be included in the architecture of the VTS Digital Services

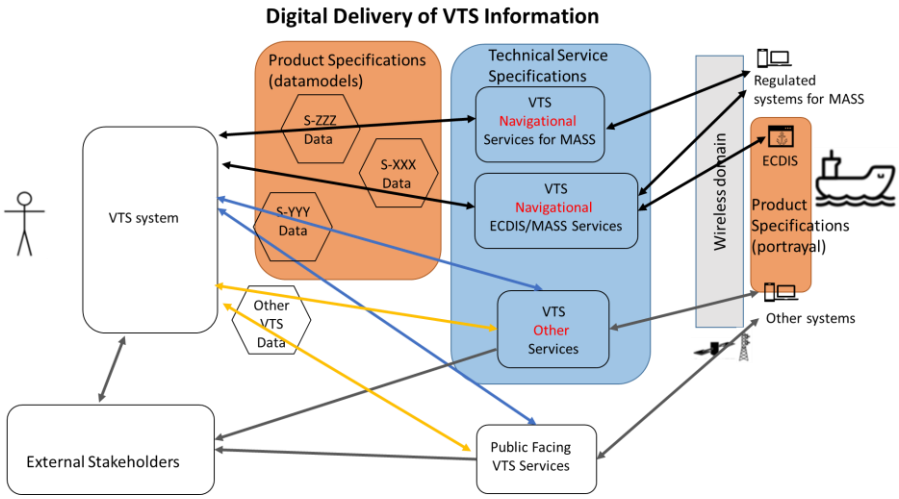
2 Take notice of the fact that VTS related data-elements from S-211 will be included in S-212 and that the developed technical services shall no longer refer to S-211

3 A liaison note to DTEC needs to be sent to make a link between the VTS Digital Services architecture and the Common Shore-based System Architecture (CSSA)

4 Progress the related documents (in annexes) during VTS54

ANNEX A: ARCHITECTURE OF THE DIGITAL DELIVERY OF VTS INFORMATION

1



Explanation

1. Purpose/scope
   a) The purpose of the drawing is to explain the high level architecture on how the technical services and the product specifications relate to facilitate a digital data exchange for VTS information
   b) It ‘s also meant to clarify to process regarding the tasks on Maritime Services, Technical Services and a Product Specification for the Digital Delivery of VTS Information including the operational aspects of these elements
   c) The data exchange to ships meet the requirements of both manned and unmanned ships
2. Definitions
   a) VTS System
      - See definition in G.1111
   b) Technical Services Specification
      - Describes how to implement the digital data exchange using specific technologies (see G.1128)
      - The technical service specifications are referenced in the MS description in the context of eNavigation for VTS as “associated technical services” (MSC.1/circ.1610)
      - VTS Navigational ECDIS/MASS Services specifications
        - This is the subset of the technical service specifications from the VTS system that is targeting ECDIS and/or regulated on board MASS systems
        - The communication between the VTS system and the ECDIS should follow set regulations, in particular IEC (IEC 63173-2:2022) and IALA (G.1157)
        - The IEC 63173-2:2022 requires a service and identity registry which can be provided by the Maritime Connectivity Platform (MCP)

- VTS Navigational Service specifications for MASS
  - This is the subset of the technical service specifications from the VTS system that is targeting regulated on board MASS systems
  - The communication between the VTS system and the MASS on board systems should follow set regulations, in particular IEC (IEC 63173-2:2022) and IALA (G.1157)
  - The IEC 63173-2:2022 requires a service and identity registry which can be provided by the Maritime Connectivity Platform (MCP)
- VTS Other Services specifications
  - This is the subset of the technical service specifications from the VTS system that is targeting other (non ECDIS) systems

c) Technical Service
- This is the implementation of a technical service specification

d) Public Facing VTS Services
- The exchange of data through other means than harmonized technical services (e.g. email, website, …)

e) S-100 Product Specifications
- S-XXX data
  - S-100 datasets exchanged with the VTS that have been mandated to be used and portrayed on the ECDIS and/or regulated on board MASS systems
- S-ZZZ data
  - S-100 datasets exchanged with the VTS that have been mandated to be used on regulated systems for MASS
- S-YYY data
  - S-100 datasets exchanged with the VTS to targeted systems other than ECDIS and/or regulated on board MASS systems
  - Some of these Product specifications may include portrayal and others might not

f) Other VTS data
- Datasets exchanged with the VTS other than S-100, these can possibly been harmonized by other standards (e.g. IMO compendium, …)

3. External Stakeholders

a) Entities other than ships that need to exchange data with the VTS
- Coastal State Authorities
- Port Authorities
- Allied Services
- Other VTS Centers
- Hydrographic/Meteorological offices
- ENC providers
- Shore Control Centers
- …

b) Data exchange with external stakeholders and other relevant entities include but is not limited to S-100 harmonized datasets

4. Tasks

a) Product Specification (task 2.3.1)

- Has 2 parts:
  - VTS exclusive datamodel based on elements in the IHO feature catalogue, i.e. not covered by Product Specifications by other domains
  - When needed definition of the portrayal

b) Technical Services Specifications (task 2.5.1)

- Making the Technical Service Specifications derived from the use cases defined by task 1.2.4

ANNEX B:

SERVICE SPECIFICATION FOR [DIGITAL] VTS TRAFFIC CLEARANCE SERVICE

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. The design of the service interfaces was adapted from the standard for Secure communication between ship and shore IEC 63173-2:2022.

1.1 Purpose of the Document

The purpose of this service specification document is to provide a holistic overview of digital VTS Traffic Clearance Service and its building blocks in a technology-independent way, according to the guidelines given in **Error! Reference source not found.**. It describes a well-defined baseline of the service by clearly identifying the service version.
The aim is to document the key aspects of the VTS Traffic Clearance Service at the logical level:

- the operational and business context of the service
  - requirements for the service (e.g., information exchange requirements)
  - involved nodes: which operational components provide/consume the service
  - operational activities supported by the service
  - relation of the service to other services
- the service description
  - service interface definitions
  - service interface operations
  - service payload definition
  - service dynamic behaviour description
- service provision and validation aspects

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. 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

This section provides an overview of activities, which are dealing with similar topics and lists already finished ones that provided inputs to this activity.'
To be added reference to Route Based VTS Service Specifications
To be added short references to IEC 63173-1:2021 – S-421, S-212 as well as S-210

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*

ID	*urn:mrn:iala:techsvc:vts:tcs* *[not official designation, for example only]*
Version	*0.23*
Description	*The VTS Traffic Clearance Service specification describes a standardized service implementing the Vessel Traffic Service traffic clearances communication between ship and shore*
Keywords	*VTS, MS1, Traffic Clearance, Ship Traffic Management, S-212, S-421*
Architect(s)	
Status	*Provisional*

3 OPERATIONAL CONTEXT

According to IMO resolution A.1158(32) Guidelines for Vessel Traffic Services one of the purposes of a VTS is to monitor and manage ship traffic to ensure the safety and efficiency of ship movements. IALA Guideline G1089 Provision of a VTS states that the monitoring and management may include among other things forward planning and prioritization of ship movements to prevent congestion or dangerous situations and improve overall efficiency, establishing a system of traffic clearances and organizing space allocation.
The Maritime Service description for MS1 Vessel Traffic Services describes user needs for digital information services for the exchange of VTS information by electronic means between a VTS and vessel. Vessels using MS1 can receive information related to the management of ship traffic in a digital format that can be displayed in the navigational equipment on board. Digital information exchange may apply to elements of vessel traffic management that is not time critical.
Traffic clearance refers to the process of ensuring that there is sufficient space and time for vessels to navigate safely through an area as well as consider other vessels, obstructions, regulatory and environmental factors. The process of traffic clearances includes the use of communication systems to inform mariners about the location and movements of other vessels and potential hazards.

3.1 Present Day Operational Context

One of the main tasks for VTS is to monitor and manage vessel traffic, including establishing a system for traffic clearances. Traffic clearances may be required in situations when a vessel is:

- entering or prior to entering a VTS area.
- departing from a berth or an anchorage within a VTS area.
- entering or prior to a fairway within a VTS area.
- prior to commencing a manoeuvre that may be detrimental to safe navigation.

Traditionally VTS communication and interaction with ships is almost exclusively undertaken by VHF voice communications. The move to digital communications will reduce the amount of VHF communication and provide timely information which will improve safe and efficient ship traffic and pave the way to future machine to machine operations.
System interfaces for digital exchange of information related to ship traffic management are not standardised. This document starts descripting these standardisations with use cases.

3.2 Envisioned Operational Context

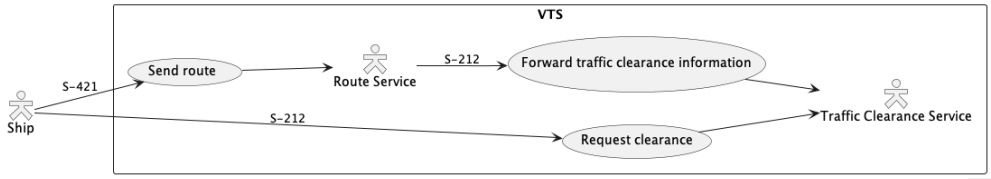
A more digitally- envisioned operational clearance system will provide several valuable benefits to improve communication and with that safety, efficiency, and sustainability. Digital systems will enhance situational awareness for the vessel and provide real-time information and help to ensure that all parties timely have the necessary information to make informed decisions and take

appropriate actions. This service paves the way for more automated services and decision support tools. Remark: To be added: Prerequisites and assumptions for the minimum use cases.

For effective Traffic Clearance Service VTS requires the knowledge of vessels intentions. The primary means to share vessels ETA and ETD times would be the sharing of vessels route plans, including schedule. If the vessel is not capable of sharing route plans, the alternative mean would be sharing only ETA and ETD times and destination of vessel. It should be ensured that the times in the different systems are aligned.

This service specification does not define the on-board systems used in for traffic clearance service. When implementing the Traffic Clearance Service which on-board system the service will be deployed on should also be planned.

It should be noted that if ECDIS will be used as an on-board the system should be compatible with the performance standards for ECDIS. IMO is currently working on the update for ECDIS PS to support the exchange of route plans. At the time of writing of this document ECDIS PS does not support the exchange of ETA/ETD timestamps, which limits the use of only timestamp-based systems to back bridge systems on-board.



The service can be used directly from ship systems or by sending route information to VTS route services that can forward and communicate the traffic clearance request to the Traffic Clearance Service. The details of this use case are not in the scope of this document however.

The service is based on standardized structured data format, that will enable the exchange of information related to traffic clearances in the VTS area.

A typical voyage through VTS area can be defined by three general use cases: departing from a berth or anchorage within a VTS area, passing through a VTS area and entering VTS area.

The following general use cases provide examples for the digital information exchange between VTS and vessels using traffic clearance service:

Use Case 1 - Departing vessels.

1. Vessel wants to leave berth/anchorage.
2. The vessel sends route plan, with schedule through its system to the service and requests traffic clearance to leave berth/anchorage.
3. VTS sends acknowledgement, updated RTD or denial which may include additional information on when vessel can leave the berth/anchorage.
4. Service delivers response to the vessel.
5. The vessel acknowledges revised ETD and sends response to the VTS.

Use Case 2 - Passing through VTS area

1. Before the vessel enters VTS area
2. The vessel sends route plan, with schedule through its system to the service and requests traffic clearance to proceed through the VTS area from the service

3. If vessel's planned route and schedule is suitable, then VTS send acknowledgement, [go to step 5]
4. If vessel's planned route or schedule is not suitable, VTS sends new recommended RTA to the vessel through the service
5. The vessel acknowledges revised ETA and sends response to the VTS
6. New route plan and schedule is acknowledged by the VTS [go to step 2]
7. The vessel enters the VTS area

Use Case 3 - Arriving vessels.

1 Before the vessel enters VTS area.
2 The vessel sends route plan, with schedule through its system to the service and requests traffic clearance to proceed to the predefined area from the service
3 If vessel's planned route and ETA is suitable, then VTS send acknowledgement
4 If vessel's planned route or ETA is not suitable, VTS sends new recommended RTA to the vessel through the service
5 The vessel acknowledges revised ETA and sends response to the VTS
6 New ETA is confirmed by the VTS
7 The vessel enters the VTS area

Figure 1 gives overwiev of the dataflows between vessels using the traffic clearance service and VTS.

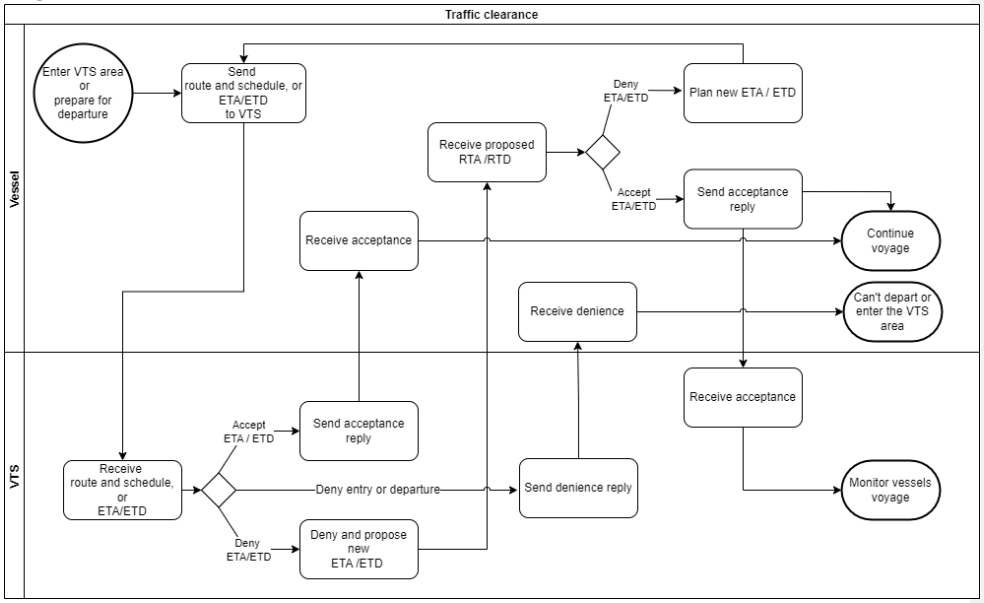


Figure 1: Traffic clearance dataflow

3.3 Functional and Non-functional Requirements

The table below lists applicable existing requirements for the Traffic Clearance service.

Table 1: Requirements Tracing

Requirement Id	Requirement Name	Requirement Text	References

Functional requirements

Requirement Id	**TCSF001**
Requirement Name	Receive ETA from vessel
Requirement Text	A vessel must be able to send its estimated time of arrival (ETA) to the service. The service must have the ability to forward the received ETA to the VTS System.
Rationale	Sending the ETA of the vessel to the service is a core requirement of the service. In most cases the ETA sent will be the ETA to port, but it could be any ETA that is needed to communicate between the vessel and VTS.
Author	

Requirement Id	**TCSF002**
Requirement Name	Receive ETD from vessel
Requirement Text	A vessel must be able to send its estimated time of departure (ETD) to the service. The service must have the ability to forward the received ETD to the VTS System.
Rationale	Sending the ETD of the vessel to the service is a core requirement of the service. In most cases the ETD sent will be the ETD from port, but it could be any ETD that is needed to communicate between the vessel and VTS.
Author	

Requirement Id	**TCSF003**
Requirement Name	Send ETA proposal to vessel from VTS
Requirement Text	The service must facilitate the sending of an ETA proposal from VTSs to the vessel. The proposal may be a part of a rejection of an ETA request from a vessel or standalone. If the proposal is a part of a rejection, the rejection message must be identified.
Rationale	When VTS personnel are either reviewing a sent ETD from a vessel or trying to organize traffic and need to suggest an ETD to a vessel the service must be able to send an ETD proposal to the vessel.
Author	

Requirement Id	**TCSF004**
Requirement Name	Send ETD proposal to vessel from VTS
Requirement Text	The service must facilitate the sending of an ETD proposal from VTSs to the vessel. The proposal may be a part of a rejection of an ETD request from a vessel or standalone. If the proposal is a part of a rejection, the rejection message must be identified.
Rationale	When VTS personnel are either reviewing a sent ETD from a vessel or trying to organize traffic and need to suggest an ETD to a vessel the service must be able to send an ETD proposal to the vessel.
Author	

Requirement Id	**TCSF005**
Requirement Name	Approve ETA/ETD from vessel
Requirement Text	The service must facilitate the sending of the acceptance of the ETA/ETD from the vessel without the need to negotiate the time. The approval may also include a new or changed location to which the ETA/ETD is defined.
Rationale	
Author	

Requirement Id	**TCSF006**
Requirement Name	Send ETA / ETD proposal from VTS to vessel
Requirement Text	It will be possible for VTSO to send new proposed estimated time of arrival (ETA) and/or estimated time of departure (ETD) to the vessel
Rationale	Even before the vessel communicates its ETA or ETD, there must be the ability to communicate a proposal from VTS to a vessel.
Author	

Requirement Id	**TCSF007**
Requirement Name	Send acknowledgement from vessel to VTS
Requirement Text	After receiving a suggested ETA/ETD from VTS to the vessel the mariner must be able to either accept the proposal and thus send an immediate acknowledgement to VTS or propose a new ETA/ETD to VTS.
Rationale	The negotiation process for a new proposed ETA/ETD may include several phases of proposed times and new counterproposals. However a final acknowledgement must also be a part of the process so that VTS knows when vessel has approved the suggested ETA/ETD.
Author	

Requirement Id	**TCSF008**
Requirement Name	Service integration with VTS System (vessel traffic management information system)
Requirement Text	The service must integrate with the VTS System so that the information received from vessels can be utilized by the VTS System.
Rationale	The exact details of how this requirement are fulfilled are left to each implementor as they depend on the functionalities of the VTS System itself. In some cases, it may be better for the VTS System to poll the service, in other cases an event may be triggered, or a simple API call on the VTS System may be used. From the perspective of this specification the implementation details of how the service integrates with the VTS System can be left open.
Author	

Requirement Id	**TCSF009**
Requirement Name	Service must support event-based communication
Requirement Text	For best possible compatibility with planned platforms service must be compatible with event driven.
Rationale	The event driven approach mimics the approach of MMS. MMS with its agents and edge routers abstracts much of the complexity of the challenges faced with ship to shore communication. An event driven approach is also architecturally different from a push/pull API-based approach. By supporting both approaches the services are as future proof as can be at the current stage.
Author	

Requirement Id	**TCSF010**
Requirement Name	Service must support API based communication
Requirement Text	Service should offer APIs for direct communication for SECOM style push/pull communication.
Rationale	Direct API communication enables many ways of interaction with the service. The interfaces defined for the API communication do not require SECOM-style implementations, but the design of the APIs is based on the requirements of SECOM.
Author	

Requirement Id	**TCSF011**
Requirement Name	Messages should be signed
Requirement Text	The service provider and consumer should sign all messages to better enable verification of the communicating parties.
Rationale	While both approaches typically allow both signed and unsigned communication, preferring signed communication enables easier verification and makes it harder to spoof sources of communication.
Author	

Non-functional requirements

Requirement Id	**TCSNF001**
Requirement Name	Authenticity
Requirement Text	The recipient of information must be able to verify the authenticity of the received datasets. The IDSec tools and identity registry specified in MCP must be used to facilitate this.
Rationale	
Author	

Requirement Id	**TCSNF002**
Requirement Name	Integrity
Requirement Text	It must be clear to both service provider and consumer whether changes have been made to the information after the dataset was created. All messages must be signed with the correct certificates so that the contents of a message can be validated.
Rationale	
Author	

Requirement Id	**TCSNF003**
Requirement Name	Availability
Requirement Text	The service must always be available with the ability defined by Owner of the service the to deliver traffic clearance information to its consumers.
Rationale	The service must be available based on the VTS Service hours and service levels.
Author	

Requirement Id	**TCSNF004**
Requirement Name	Performance – timeliness
Requirement Text	The service must provide a response to an incoming request instantly. This response is by necessity a technical delivery acknowledgement and not a business process response. This applies both to requests coming from vessels and VTS System.
Rationale	Especially from a vessel's point of view it is important to get an acknowledgement that the service has received a request so that the vessel's system does not need to try resending the request.
Author	

Requirement Id	**TCSNF005**
Requirement Name	Reliability
Requirement Text	The service must provide a retry mechanism to ensure that messages are delivered to the vessel or VTS System even if the first request fails.
Rationale	As the service is effectively a proxy between the VTS System and vessel's systems it is vital that message delivery to the real consumer is ensured by retrying sending the message. This is of increased importance when the vessel is behind an unreliable network connection or the actual data carrier changes during messaging.
Author	

3.4 Other Constraints

3.4.1 Relevant Industrial Standards

To be added a table of applicable industrial standards

3.4.2 Operational Nodes

The following tables describe the operational nodes of the service.

Table x: Operational Nodes providing the Traffic Clearance service

Operational Node	**Remarks**
Vessel	Vessels sailing in a service coverage area.
VTS centres	VTS centres responsible for a service coverage area.

3.4.3 Operational Activities

Optional. If an operational model exists and provides sufficient details about operational activities, then this section shall include a mapping of the service to the relevant operational activities.

Table x: Operational Activities supported by the XYZ service

Operational Activity	**Remarks**

4 SERVICE OVERVIEW

4.1 Service Interfaces

Communication between ship and service is done either via APIs or an event-based approach. The selection of the respective approach is a service design level decision.
And event-based service is based on an event (or message) driven architecture. All calls are assumed to be asynchronous with only a response receipt given from shore to ship or ship to shore.

In the API based approach the service provider is the ship itself because communication is primarily initiated by the ship and the ship is the primary source of the pushed messages. The consumer in this case is most likely the VTS system.

5 SERVICE DATA MODEL

The service must consume a data model that is a direct subset of S-212.
For complete and updated documentation of the S-212 data model refer to the latest S-212 Product Specification which can be found at IALA S-200 Data modelling web site https://www.iala-aism.org/technical/data-modelling/iala-s-200-development-status/s-212/
The data transfer between service and consumers MUST always conform to the model displayed below. Fields that are optional are identified with MAY and SHOULD in the descriptions below.
Everything below this requires changes once the S-212 model is understood well enough to define usable elements and what additions are needed!
This data model does not define the envelopes in which the data is sent between the ship and VTS system or all of the interface parameters. This only defines the subset of S-212 data that must be supported by the service.

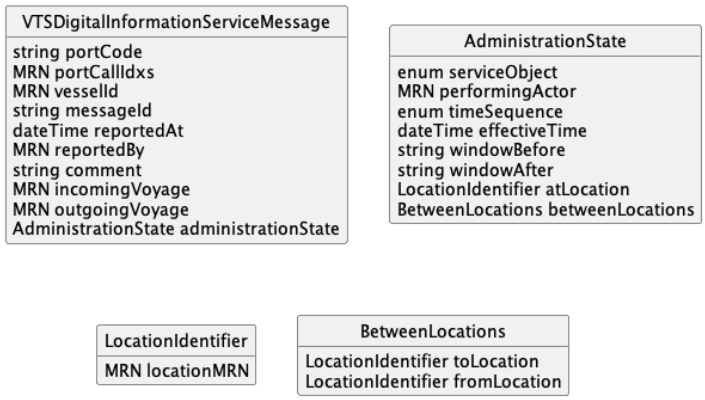


Figure 2: Traffic clearance data model diagram

The description of the data model is as follows:

- Must be one of:
  - portCallIdentifier – MRN and preferred if known.
  - portCode – UN/LOCODE as per standard, used when portCallIdentifier is not available
- vesselId – vessel MRN, IMO SHOULD be preferred, but MMSI MAY also be used.
- messageId – MRN + UUID to uniquely identify the message across systems.
- reportedAt – SHOULD be used as timestamp of message creation.
- reportedBy – SHOULD be used to identify the MRN or other identity of the person sending the message, for audit trails etc
- comment – MAY be used to pass additional information as part of the message for human consumption.
- incomingVoyage / outgoingVoyage – SHOULD be used to identify route the is shared or to ensure that all communication on a single arrival / departure is easily connected to a specific journey. Remark: Should be validated as URI
- administrationState

- serviceObject – Must be one of: Arrival Anchoring Operation, Arrival Berth, Arrival Portarea, Arrival Vtsarea, Departure Anchoring Operation, Departure Berth, Departure Portarea, Departure Vtsarea, Pilotage, Port Visit, Ready to Sail Operation
- performingActor – if used, must be MRN of vessel
- effectiveTime – timestamp of the ETA/ETD being communicated.
- windowBefore / windowAfter – MAY be used to give relative offset of the window requested / given. In hh:mm format.
- timeSequence – MUST be one of Cancelled, Confirmed, Denied, Requested, or Request Received
- One of
  - atLocation
    - locationMRN – MRN specifying the point of arrival or departure. This may be changed by VTS / port operator to indicate a recommended location instead of the location sent by ship.
  - betweenLocations
    - toLocation / fromLocation – MRN specifying the point from and to the clearance message refers to.

6 SERVICE INTERFACE SPECIFICATIONS

The Service Interfaces are dependent on the technical design and out of scope of this specification. This paragraph will be adjusted or completely removed according to the future changes in G1128.

7 SERVICE DYNAMIC BEHAVIOUR

This section describes the interactive behaviour of the traffic clearances between ship and shore. Before the exchange of information is initiated, the service consumer retrieves the identity of the service provider from the service infrastructure and performs authentication procedure. If not authenticated, the service request is rejected. The specific authentication procedure is out of scope of the service specification and is described in the technical designs of this service.
This section will be added later.

8 REFERENCES

Nr.		Version	Reference
1	IALA Guideline G1128	ED 1.4	THE SPECIFICATION OF E-NAVIGATION TECHNICAL SERVICES
2	IALA Recommendation R1023	ED 1.0	MARITIME RESOURCE NAMES
3	IHO Standard S-100	ED 5.0.0	IHO Universal Hydrographic Data Model https://iho.int/uploads/user/pubs/standards/s-100/S-100_5.0.0_Final_Clean_Web.pdf
4	IEC 63173-2 ED1	1.0	Maritime navigation and radiocommunication equipment and systems – Data interfaces – Part 2: Secure communication between ship and shore (SECOM)

Nr.	Version	Reference
5 IALA data model S-212	XX	IALA VTS Digital Information Service Product Specification

FIGURE 1 **ACRONYMS AND TERMINOLOGY**

a. Acronyms

Term	Definition
API	Application Programming Interface
MC	Maritime Cloud
MEP	Message Exchange Pattern
MRN	Maritime Resource Name
NAF	NATO Architectural Framework
REST	Representational State Transfer
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSD	Service Specification Document
UML	Unified Modelling Language
URL	Uniform Resource Locator
VTS	Vessel Traffic Service
WSDL	Web Service Definition Language
XML	Extendible Mark-up Language
XSD	XML Schema Definition

b. Terminology

Term	Definition
External Data Model	Describes the semantics of the "maritime world" (or a significant part thereof) by defining data structures and their relations. This could be at logical level (e.g., in UML) or at physical level (e.g., in XSD schema definitions), as for example standard data models, or S-100 based data produce specifications.
Message Exchange Pattern	Describes the principles how two different parts of a message passing system (in our case: the service provider and the service consumer) interact and communicate with each other. Examples: In the Request/Response MEP, the service consumer sends a request to the service provider in order to obtain certain information; the service provider provides the requested information in a dedicated response. In the Publish/Subscribe MEP, the service consumer establishes a subscription with the service provider in order to obtain certain information; the service provider publishes information (either in regular intervals or upon change) to all subscribed service consumers.
Operational Activity	An activity performed by an operational node. Examples of operational activities in the maritime context are: Route Planning, Route Optimization, Logistics, Safety, Weather Forecast Provision, …
Operational Model	A structure of operational nodes and associated operational activities and their inter-relations in a process model.
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 stations, 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 Design Description	Documents the details of a service technical design (most likely documented by the service implementer). The service design description includes (but is not limited to) a service physical data model and describes the used technology, transport mechanism, quality of service, etc.
Service Implementation	The provider side implementation of a dedicated service technical design (i.e., implementation of a dedicated service in a dedicated technology).
Service Implementer	Implementers of services from the service provider side and/or the service consumer side. Anybody can be a service implementer but mainly this will be commercial companies implementing solutions for shore and ship.
Service Instance	One service implementation may be deployed at several places by same or different service providers; each such deployment represents a different service instance, being accessible via different URLs.
Service Instance Description	Documents the details of a service implementation (most likely documented by the service implementer) and deployment (most likely documented by the service provider). The service instance description includes (but is not limited to) service technical design reference, service provider reference, service access information, service coverage information, etc.
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 stations, organizations (e.g., meteorological), commercial service providers, etc.
Service Specification	Describes one dedicated service at logical level. The Service Specification is technology-agnostic. The Service Specification includes (but is not limited to) a description of the logical operations with their data in a subset of S-212. The logical data model of the service is a subset of S-212.
Service Specification Producer	Producers of service specifications in accordance with the service documentation guidelines.
Service Technical Design	The technical design of a dedicated service in a dedicated technology. One service specification may result in several technical service designs, realising the service with different or same technologies.
Service Technology Catalogue	List and specifications of allowed technologies for service implementations. Currently, SOAP and REST are envisaged to be allowed service technologies. The service technology catalogue shall describe in detail the allowed service profiles, e.g., by listing communication standards, security standards, stacks, bindings, etc.
Spatial Exclusiveness	A service specification is characterised as “spatially exclusive”, if in any geographical region just one service instance of that specification is allowed to be registered per technology. The decision, which service instance (out of a number of available spatially exclusive services) shall be registered for a certain geographical region, is a governance issue.

ANNEX C: SERVICE DESIGN DESCRIPTION FOR THE S-421 ROUTE PLAN SERVICE

<REST Technology according to SECOM>

1 INTRODUCTION

This design is intended to support all of the different Service Specifications that will be create where Route Exchange is involved.

The data product exchanged in this design is S-421 Route Plan.

The service can be part of a service orchestrated architecture.

1.1 Purpose of the Document

The purpose is to describe the design of service specification as a REST service that facilitates development of service instances.

1.2 Intended Readership

This service design description document is intended to be read by service architects, designers, system engineers and developers.

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

1.3 Inputs from Other Sources

This section provides an overview of activities, which are dealing with similar topics and lists already finished ones that provided inputs to this activity.

2 SERVICE DESIGN IDENTIFICATION

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

Table 1 ***Service Design Identification***

Name	Route Exchange REST Service Design
ID	Urn:mrn:iala:techsvc:design:routeexchange
Version	0.0.1
Technology	REST
Service Specification ID	Reference to the service specification
Service Specification Version	Reference to the service specification
Description	Service design to exchange route plans
Keywords	Route Plan, Route Exchange
Architect(s)	IALA TG 2.
Status	Provisional

3 TECHNOLOGY INTRODUCTION

3.1 Service technology and service transportation protocol

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

REST is an architectural style, and an approach to communications that is often used in the development of Web services. The use of REST in SECOM is preferred over other more heavyweight protocols such as e.g. SOAP (Simple Object Access Protocol) because REST does not leverage as much bandwidth, which makes it a better fit for use in communication between vessels and shore based representation of the same.

REST, which typically runs over HTTP (Hypertext Transfer Protocol), has several architectural constraints:

- Decoupling – Decouples consumers from producers which suits SECOM decentralized architecture well.
- Stateless existence – Also a good prerequisite for a decentralized architecture design.
- Able to leverage a cache – Probably less important in SECOM since most of the interaction is between machines, although for services with man-machine interfaces this is of importance.
- Leverages a layered system – SECOM is dependent on good scaling capabilities which REST supports.
- Leverages a uniform interface – Again since SECOM defines the available services centrally in one or several Service registry(s) this constraint supports implementations being decoupled from the services they provide.

The definition of each operation defines additional error messages that the operation specifically shall respond with as a complement to the HTTP response codes defined by HTTP/1.1 (RFC 7231).

3.2 Security

3.2.1 Communication channel security

When consuming service instances according to SECOM, the internet transport shall be protected with TLS and valid certificates from trusted party as stated in SECOM communication channel security. The protection of the channel is a complement to the protection of the data itself and is necessary to be included to secure also other service requests, such as subscription request, access request and notifications. The SECOM communication channel security describes the usage of certificate obtained from a trusted identity registry and thereby enables authentication on the service interaction itself as depicted in Figure 3.

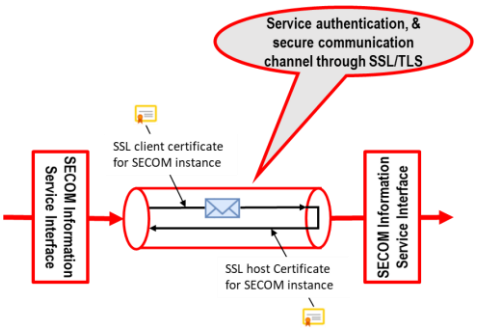


Figure 3 - Secure communication channel

The SECOM communication channel security relies on a SECOM Public Key Infrastructure (SECOM PKI) or Public-Private Key management using X.509 Certificates to exchange the keys.

The SECOM communication channel security scheme does not comprise the "last mile" links between the SECOM information service interface and the end-user application. In **Error! Reference source not found.** there are informative examples and guidance of how such protection could be achieved.

4 SERVICE DESIGN OVERVIEW

4.1 General

This service design is based on SECOM Service Design Template 0 and from that the service interfaces relevant for S-421 have been chosen. This service design is intended to be used by any actor independent on purpose of exchanging the S-421 Route Plan, hence all interfaces from the SECOM Service Design Template are described here.

4.2 Service Interfaces

This chapter is based on the description in ref 0 and ref 0 and only describes the additional information required to tailor the service interface to S-421 Route Plan data.

Table 1 gives an overview of the service interface and operations that constitutes the S-421 SECOM information service.

Table 1 – S-421 Service interface overview

Operation	Exchange Pattern	Definition
Upload	ONE_WAY	Interface to send (push) S-421 to consumer
Acknowledgement	ONE_WAY	Interface to send acknowledgement on uploaded information.
Get	REQUEST_RESPONSE	Interface to ask for (pull) S-421 Route Plans from provider
Get Summary	REQUEST_RESPONSE	Interface to ask for (pull) a list of available S-421 Route Plans from provider
Subscription	PUBLISH_SUBSCRIBE	Interface to create subscription of S-421 Route Plans

Remove Subscription	ONE_WAY	Interface to remove subscription on S-421 Route Plans
Subscription Notification	ONE_WAY	Interface for notification from subscription events
Access	REQUEST_CALLBACK	Interface to ask for access to S-421 Route Plans
Access Notification	ONE_WAY	Interface for notification from access request
Capability	REQUEST_RESPONSE	Interface to ask for the interface capabilities. Mandatory to implement.
Ping	REQUEST_RESPONSE	Interface to check status on the service instance. Mandatory to implement.
Encryption Key	ONE_WAY, REQUEST_CALLBACK	Interface to securely send symmetric key for data encryption
PublicKey	ONE_WAY, REQUEST_RESPONSE	Interface to request (pull) and send (push) a public certificate

5 PHYSICAL DATA MODEL

[Source IEC 63173-1 S-421]
Refer to URL for XSD file to S-421
Refer to IEC 63173-1 Route Plan

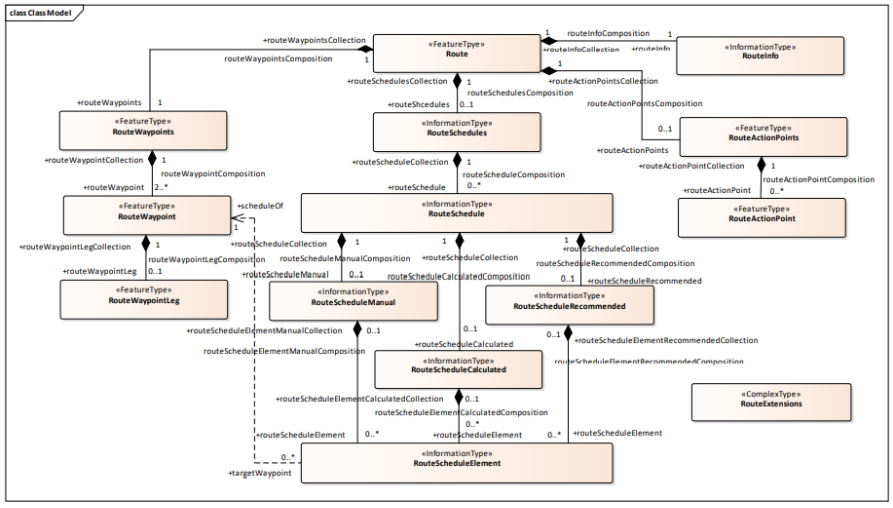


Figure 1 – Route Plan application schema

Figure 1 <Service Name> Service Data Model diagram

An XML schema for this data model is included in the formal service design xml file attached in 11.

6 SERVICE INTERFACE DESIGN

This section describes the details of each service interface and its operations.

The Service Interface design covers the static design description while the dynamic design (behaviour) is described in section 7.

6.1 Service Interface S-421 Route Plan SECOM Service

The following definitions of the interface and operations are based on SECOM Service Design Template, see ref 0.

Each operation has been added with a section for the specific S-421 Route Plan service details as complement to the design template information.

6.1.1 Operation UPLOAD

This interface is called when client uploads (pushes) data to the service. The sender (client) decides format and protection of the data. If acknowledgement is requested it will be given by callback to interface Acknowledgement.

The purpose with this interface is to upload (push) information that shall not be larger than a maximum size of 350kb (Base64 encoded) to an information consumer. An information consumer shall implement this interface in order to receive information.

6.1.1.1 Operation Functionality

TBD

6.1.1.2 Operation Parameters

POST baseUrl/v1/object {body} : response

The data (payload) package with its metadata.

Attribute	Type	Format	Require
envelope data	string	Base64	Required
envelope containerType	integer	enum	Required
envelope dataProductType	integer	enum	Required
envelope exchangeMetadata dataProtection	boolean		Required
envelope exchangeMetadata protectionScheme	string		Required
envelope exchangeMetadata dataSignatureReference	string		Required
envelope exchangeMetadata dataSignatureValue publicRootCertificateThumbprint	string	SHA1	Optional
envelope exchangeMetadata dataSignatureValue publicCertificate	string	Minified PEM	Required

Commented [MO1]: Check if this is correct

envelope exchangeMetadata compressionFlag	boolean		Required
envelope fromSubscription	boolean		Optional
envelope ackRequest	boolean		Required
envelope transactionIdentifier	string	uuid	Required
envelope envelopeSignatureCertificate	string	Minified PEM	Required
envelope envelopeRootCertificateThumbprint	string	SHA1	Optional
envelope envelopeSignatureTime	string	date-time	Optional
envelopeSignature	string	HEX	Required

Table 2 Service body

Response Code	Object	Type	Description
200	message	string	Message successfully uploaded
	Secom_ResponseCodeEnum	integer	
400	message	string	Bad request
401	message	string	Unauthorized
403	message	string	Not authorized to upload link
405	message	string	Method not allowed
500	message	string	Internal server error
501	message	string	Not implemented

Table 3 Service response

6.1.1.3 Values for S-421 Route Exchange Service

The default value for data is one base64 encoded S-421 XML message.

The default value for containerType is S100_DataSet.

The dataProductType is 24/25 for S421 Route plan.

The default value for dataProtection is false, the S-421 Route Plan is not encrypted, but it can optionally be set to true if encrypted. The the encryptionKey must also be exchanged.

The default value for protectionScheme is “SECOM”.

The dataSignatureReference is “DSA”.

The default value for compressionFlag is false, but optionally it can be set to true if the data is instead a base64 encoded ZIP compressed S421 XML message.

If the S-421 Route Plan has been uploaded within a subscription, the subscriptionFlag is set to true.

6.1.2 Operation GET

This interface is called when client gets (pulls) data from the service.

The Get interface is used for pulling information from a service provider. The owner of the information (provider) is responsible for the authorization procedure before returning information. The consumer

can ask for information by its reference, geometry, time or arbitrary query for e.g. status on the information product. If no filtering parameters are given, all authorized information is to be sent. The information owner decides what information the consumer is authorized to based on the identity in the TLS client certificate i.e. the identity the service instance belongs to.

6.1.2.1 Operation Functionality

TBD

6.1.2.2 Operation Parameters

GET baseUrl/v1/object/pathParams?queryParams : response

Attribute	Type	Format	Require
dataReference	string	uuid	optional
containerType	integer	enum	optional
dataProductType	integer	enum	optional
productVersion	string		optional
geometry	string	WKT	optional
unlocode	string	[A-Z]{5}	optional
validFrom	string	date-time	optional
validTo	string	date-time	optional
page	integer		optional
pageSize	integer		optional

Table 4 Service parameter

HTTP Code	Content	Type	Description
200	application/json	string	The operation was performed successfully
	array of {		
	data	string	
	exchangeMetadata dataProtection	boolean	True if data encrypted
	exchangeMetadata protectionScheme	string	Reference to protection schema administrator
	exchangeMetadata digitalSignatureReference	string	
	exchangeMetadata digitalSignatureValue publicRootCertificateThumbprint	string	
	exchangeMetadata digitalSignatureValue publicCertificate	string	
	exchangeMetadata digitalSignatureValue digitalSignature	string	
	exchangeMetadata compressionFlag	boolean	True if compressed
	ackRequest	integer	
	}		

	pagination totalItems	integer	
	pagination maxItemsPerPage	integer	
400	application/json	string	Bad request
401	application/json	string	Unauthorized
403	application/json	string	Not authorized to requested information
404	application/json	string	Information not found
405	application/json	string	Method not allowed
500	application/json	string	Internal server error
501	application/json	string	Not implemented

Table 5 Service response

6.1.2.3 Values for S-421 Route Exchange Service

TBD

6.1.3 Operation UPLOAD LINK

The purpose with this interface is to upload (push) a link to information to a consumer. Hence, a consumer shall implement this interface in order to receive a link to the information that can be retrieved. This interface shall be used when large amount of data shall be exchanged. The provider of information then uploads a link to a consumer, and the consumer then use the Get by Link interface to pull the data from the provider.

Use this when data is larger than allowed with POST in REST.

6.1.3.1 Operation Functionality

TBD

6.1.3.2 Operation Parameters

POST baseUrl/v1/object {body} : response

The message link with its metadata

Attribute	Type	Format	Require
envelope containerType	integer	enum	required
envelope dataProductType	integer	enum	required
envelope exchangeMetadata dataProtection	boolean		required
envelope exchangeMetadata protectionScheme	string		required
envelope exchangeMetadata dataSignatureReference	string		required
envelope exchangeMetadata dataSignatureValue	string	SHA1	optional
envelope exchangeMetadata publicRootCertificateThumbprint	string	Minified PEM	required

dataSignatureValue			
publicCertificate			
envelope	boolean		required
exchangeMetadata			
compressionFlag			
envelope	boolean		optional
fromSubscription			
envelope	integer	enum	required
ackRequest			
envelope	string	uuid	required
transactionIdentifier			
envelope	string	Minified PEM	required
envelopeSignatureCertificate			
envelope	string	SHA1	optional
envelopeRootCertificateThumbprint			
envelope	integer		optional
size			
envelope	string	date-time	required
timeToLive			
envelope	string	date-time	optional
envelopeSignatureTime			
envelopeSignature	string	HEX	required

Table 6 Service body

Attribute	Type	Format
N/A		

Table 7 Service parameters

Response Code	Content	Object	Type	Format	Description
200	application/json	message	string		Link successfully uploaded
		Secom_ResponseCodeEnum	integer		
400	application/json	message	string		Bad request
401	application/json	message	string		Unauthorized
403	application/json	message	string		Not authorized to upload link
405	application/json	message	string		Method not allowed
500	application/json	message	string		Internal server error
501	application/json	message	string		Not implemented

Table 8 Service response

6.1.3.3 Values for S-421 Route Exchange Service

TBD

6.1.4 Operation GET BY LINK

This interface is called when client downloads (pulls) large data by reference given from interface Upload Link.

The Get By Link interface is used for pulling information from a data storage handled by the information owner. The link to the data storage can be exchanged with Upload Link interface. The owner of the information (provider) is responsible for relevant authentication and authorization procedure before returning information.

6.1.4.1 Operation Functionality

TBD

6.1.4.2 Operation Parameters

GET baseUrl/v1/object/link/pathParam?queryParam : response

Param		Type	Format	Require
transactionIdentifier	query	string	uuid	required

Table 9 Service parameters

Response Code	Content	Type	Format	Description
200	application/octet-stream	string	byte	The operation was performed successfully
200	application/json	string	byte	
400	application/octet-stream			Bad request
400	application/json			
401	application/octet-stream			Unauthorized
401	application/json			
403	application/octet-stream			Not authorized to requested information
403	application/json			
404	application/octet-stream			Information with reference *dataReference* not found
404	application/json			
405	application/octet-stream			Method not allowed
405	application/json			
500	application/octet-stream			Internal server error
500	application/json			
501	application/octet-stream			Not implemented
501	application/json			

Table 10 Service response

6.1.4.3 Values for S-421 Route Exchange Service

TBD

6.1.5 Operation ACKNOWLEDGEMENT

This interface is called as response to Acknowledgement request in Upload.

During upload of information, an acknowledgement can be requested which is expected to be asynchronously received when the uploaded message has been delivered to the end system (technical acknowledgement), and an acknowledgement when the message has been opened and/or processed by the end user (operational acknowledgement). The acknowledgement contains a reference to the object delivered and has no time limit.

6.1.5.1 Operation Functionality

6.1.5.2 Operation Parameters

POST baseUrl/v1/acknowledgement {body} : response

Object with reference to information and time when delivered

Body	Type	Format	Require
envelope createdAt	string	date-time	required
Envelope envelopeCertificate	string	Minified PEM	required
Envelope envelopeRootCertificateThumbprint	string	SHA1	required
Envelope transactionIdentifier	string	uuid	required
Envelope ackType	integer	enum	required
Envelope nackType	integer	enum	optional
Envelope envelopeSignatureTime	string	date-time	required
digitalSignature	string	HEX	required

Table 11 Service body

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
	message	string		
	SECOM_code	integer	enum	
400	application/json	string		Bad request
401	application/json	string		Unauthorized
403	application/json	string		Not authorized to upload ACK
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 12 Service response

6.1.5.3 Values for S-421 Route Exchange Service

TBD

6.1.6 Operation GET SUMMARY

This interface is called when client wants a summary of available data from the service. The actual data is retrieved (pulled) using the interface Get.

A list of information shall be returned from this interface. The summary contains identity, status, size and a short description of each information object. The actual information object shall be retrieved using the Get interface. The consumer can ask for information by geometry, location and time. If no filtering parameters are given, available summary information is to be sent.

6.1.6.1 Operation Functionality

6.1.6.2 Operation Parameters

GET baseUrl/v1/object/summary/pathParam?queryParam : response

Param	Param	Type	Format	Require
containerType	query	integer	enum	optional
dataProductType	query	integer	enum	optional
productVersion	query	string		optional
geometry	query	string	WKT	optional
unlocode	query	string	5[A-Z]	optional
validFrom	query	string	date-time	optional
validTo	query	string	date-time	optional
page	query	integer		optional
pageSize	query	integer		optional

Table 13 Service parameters

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
	array of {			
	informationSummaryObject dataReference	string		
	informationSummaryObject dataProtection			
	informationSummaryObject dataCompression			
	informationSummaryObject containerType	integer	enum	
	informationSummaryObject dataProductType	integer	enum	
	informationSummaryObject info_productVersion	string		
	informationSummaryObject info_identifier	string		
	informationSummaryObject info_name	string		
	informationSummaryObject info_Status	string		
	informationSummaryObject info_Description	string		
	informationSummaryObject info_lastModifiedDate	string	date-time	
	informationSummaryObject info_size	string	integer	

	}		
	pagination totalItems	integer	
	pagination maxItemsPerPage	integer	
400	application/json	string	Bad request
401	application/json	string	Unauthorized
405	application/json	string	Method not allowed
500	application/json	string	Internal server error
501	application/json	string	Not implemented

Table 14 Service response

6.1.6.3 Values for S-421 Route Exchange Service

TBD

6.1.7 Operation ACCESS

This interface is called when client asks for access to data from the service. Response is given by callback to interface Access Notification.

Access to information can be requested through the Access interface. The result is sent asynchronously through the Access Notification interface.

6.1.7.1 Operation Functionality

TBD

6.1.7.2 Operation Parameters

POST baseUrl/v1/access {body} : response

Description of reason for requesting access to information

Body	Type	Format	Require
reason	string		required
reasonEnum	integer	enum	required
containerType	integer	enum	optional
dataProductType			optional
dataReference	string		optional
productVersion	string		optional

Table 15 Service body

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
		integer		
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error

501	application/json	string	Not implemented

Table 16 Service response

6.1.7.3 Values for S-421 Route Exchange Service

TBD

6.1.8 Operation ACCESS NOTIFICATION

This interface is called as callback response to interface Access.
Result from Access Request shall be sent asynchronous through this interface.

6.1.8.1 Operation Functionality

TBD

6.1.8.2 Operation Parameters

POST baseUrl/v1/access/ notification {body} : response

Result from the request for access; True or False

Body	Type	Format	Require
decision	boolean		required
decisonReason	string		required
transactionIdentifier	string	uuid	required

Table 17 Service body

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
	SECOM_code	integer	enum	
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 18 Service response

6.1.8.3 Values for S-421 Route Exchange Service

TBD

6.1.9 Operation SUBSCRIPTION

This interface is called when client or server initiates subscription on data from the service.
Response is given as callback to interface Upload and Subscription Notification.

The purpose of the interface is to request subscription on information, either specific information according to parameters, or the information accessible upon decision by the information provider. Each subscription request reflects one parameter query set.

6.1.9.1 Operation Functionality

TBD

6.1.9.2 Operation Parameters

POST baseUrl/v1/ subscription {body} : response

Specific id on the information object subscription is requested for specific status on the information or specific area of interest

Body	Type	Format	Require
containerType	integer	enum	optional
geometry	string		optional
unlocode	string		optional
dataProductType	integer	enum	optional
productVersion	string		optional
dataReference	string		optional
subscriptionPeriodStart	string	date-time	optional
subscriptionPeriodEnd	string	date-time	optional

Table 19 Service body

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
	message	string		
	subscriptionIdentifier	string	uuid	
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 20 Service response

6.1.9.3 Values for S-421 Route Exchange Service

TBD

6.1.10 Operation SUBSCRIPTION NOTIFICATION

This interface is called as callback response from interface Subscription or Remove Subscription.

The interface receives notifications when subscription is created or removed by information producer.

6.1.10.1 Operation Functionality

TBD

6.1.10.2 Operation Parameters

POST baseUrl/v1/subscription/notification {body} : response

Contains the identity of the information object in focus and type of event; Create or Delete.

Body	Type	Format	Require
subscriptionIdentifier	string	uuid	required
eventEnum	integer	enum	required

Table 21 Service body

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
	message	string		
	subscriptionIdentifier	string	uuid	
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 22 Service response

6.1.10.3 Values for S-421 Route Exchange Service

TBD

6.1.11 Operation REMOVE SUBSCRIPTION

This interface is called when client or server removes subscription. Response is given as callback to interface Subscription Notification.
Subscription(s) can be removed either internally by information owner, or externally by the consumer. This interface shall be used by the consumer to request removal of subscription.

6.1.11.1 Operation Functionality

TBD

6.1.11.2 Operation Parameters

DELETE baseUrl/v1/ subscription {body} : response

Specific identity of the information object to remove subscription for. If no id entity provided, all subscriptions for the caller is removed

Body	Type	Format	Require
subscriptionIdentifier	string	uuid	required

Table 23 Service body

HTTP Code	Content	Type	Format	Description
200	application/json	string		The operation was performed successfully
	message	string		Subscription *identifier* removed
400	application/json	string		Bad request
401	application/json	string		Unauthorized
403	application/json	string		Not authorized to remove subscription
404	application/json	string		Subscription *identifier* not found
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 24 Service response

6.1.11.3 Values for S-421 Route Exchange Service

TBD

6.1.12 Operation CAPABILITY

This interface is called when client asks for the service capabilities.
The purpose of the interface is to provide a dynamic method to ask a service instance at runtime what interfaces that are accessible, and what payload formats and version that are valid.

6.1.12.1 Operation Functionality

TBD

6.1.12.2 Operation Parameters

GET baseUrl/v1/capability/pathParam?queryParam : response

HTTP Code	Content	Type	Format	Description
200	application/json			The operation was performed successfully
	array of CapabilityObject {			
	dataProductType	integer	enum	
	containerType	integer	enum	
	productSchemaUrl	string		
	serviceVersion	string		
	implementedInterfaces upload	boolean		
	implementedInterfaces uploadLink	boolean		

	implementedInterfaces get	boolean	
	implementedInterfaces getByLink	boolean	
	implementedInterfaces getSummary	boolean	
	implementedInterfaces subscription	boolean	
	implementedInterfaces access	boolean	
	implementedInterfaces encryptionKey	boolean	
	}		
400	application/json	string	Bad request
401	application/json	string	Unauthorized
405	application/json	string	Method not allowed
500	application/json	string	Internal server error
501	application/json	string	Not implemented

Table 25 Service response

6.1.12.3 Values for S-421 Route Exchange Service

TBD

6.1.13 Operation PING

This interface is called when client checks the availability of the service.

The purpose of the interface is to provide a dynamic method to ask for the technical status of the specific service instance.

6.1.13.1 Operation Functionality

TBD

6.1.13.2 Operation Parameters

GET baseUrl/v1/ping**/ pathParam?queryParam : response**

HTTP Code	Content	Type	Format	Description
200	application/json			The operation was performed successfully
	message	string		Response message
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 26 Service Response

6.1.13.3 Values for S-421 Route Exchange Service

TBD

6.1.14 Operation ENCRYPTIONKEY

This interface is called when sending (pushing) encryption key to a receiver.

6.1.14.1 Operation Functionality

TBD

6.1.14.2 Operation Parameters

POST baseUrl/v1/encryptionKey {body} : response

Object with symmetric encryption key

Body	Type	Format	Require
envelope encryptionKey	string	byte	required
envelope iv			required
envelope transactionIdentifier	string	uuid	optional
envelope digitalSignatureValue publicRootCertificateThumbprint	string	SHA1	optional
envelope digitalSignatureValue publicCertificate	string	PEM	required
envelope digitalSignatureValue digitalSignature	string	HEX	required
envelope envelopeSignatureCertificate	string	PEM	required
envelope envelopeRootCertificateThumbprint	string	SHA1	required
envelope envelopeSignatureTime	string	date-time	required
envelopeSignature	string	HEX	required

Table 27 Service body

HTTP Code	Content	Type	Format	Description
200	application/json			The operation was performed successfully
	message	string		Response message
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 28 Service response

6.1.14.3 Values for S-421 Route Exchange Service

TBD

6.1.15 Operation ENCRYPTIONKEY NOTIFICATION

This interface is called when sending (pushing) encryption key to a receiver.

The purpose of this interface is to receive a request for an exchange of an encrypted secret key. The response is sent asynchronously through the consumer's POST encryption key operation.

6.1.15.1 Operation Functionality

TBD

6.1.15.2 Operation Parameters

POST baseUrl/v1/encryptionKey/notify {body} : response

EncryptionKey notification object

Body	Type	Format	Require
envelope dataReference	string	uuid	required
envelope publicCertificate	string	PEM	required
envelope envelopeSignatureCertificate	string	PEM	required
envelope envelopeSignatureTime	string	date-time	required
envelopeSignature	string	HEX	required

Table 29 Service body

HTTP Code	Content	Type	Format	Description
202	application/json			Request accepted
	message	string		Response message
	SECOM_Code	integer	enum	
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 30 Service response

6.1.15.3 Values for S-421 Route Exchange Service

TBD

6.1.16 Operation GET PUBLICKEY

This interface is called when client gets (pulls) the public certificate(s) from the service.

The purpose of the interface is to request a public key.

6.1.16.1 Operation Functionality

TBD

6.1.16.2 Operation Parameters

GET baseUrl/v1/PublicKey/pathParam?queryParam : response

Param	REST	Type	Format	Require
dataProtection	queryParam	boolean		optional
certificateThumbprint	queryParam	string	SHA	optional

Table 31 Service parameters

HTTP Code	Content	Type	Format	Description
200	application/json			The operation was performed successfully
	publicCertificate	string		PEM
400	application/json	string		Bad request
401	application/json	string		Unauthorized
403	application/json	string		Not authorized to requested information
404	application/json	string		Public key not found
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 32 Service Response

6.1.16.3 Values for S-421 Route Exchange Service

TBD

6.1.17 Operation UPLOAD PUBLICKEY

tbd

The purpose of the interface is to upload a public key.

6.1.17.1 Operation Functionality

TBD

6.1.17.2 Operation Parameters

POST baseUrl/v1/PublicKey { body } : response

Public certificate x.509 in PEM format, Base64 encoded byte array.

Body	Type	Format	Require
publicCertificate	string	PEM	

Table 33 Service body

HTTP Code	Content	Type	Format	Description
200	application/json			The operation was performed successfully
400	application/json	string		Bad request
401	application/json	string		Unauthorized
405	application/json	string		Method not allowed
500	application/json	string		Internal server error
501	application/json	string		Not implemented

Table 34 Service response

6.1.17.3 Values for S-421 Route Exchange Service

TBD

7 SERVICE DYNAMIC BEHAVIOUR

To be discussed: Add information here in this document or refer to IEC 63173-2?

8 DEFINITIONS

The definitions of terms used in this IALA Guideline can be found in the International Dictionary of Marine Aids to Navigation (IALA Dictionary) at http://www.iala-aism.org/wiki/dictionary and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary shall be considered as the authoritative source of definitions used in IALA documents.

E 8.1 TERMINOLOGY

Persons producing the Technical Service are invited to add definitions to the following list as appropriate.

Table 2 Definition of terminology – Technical Service

Term	Definition
External Data Model	Describes the semantics of the 'maritime world' (or a significant part thereof) by defining data structures and their relations. This could be at logical level (e.g. in UML) or at physical level (e.g. in XSD schema definitions), as for example standard data models, or S-100 based data produce specifications.

Term	Definition
Message Exchange Pattern	Describes the principles two different parts of a message passing system (in our case: the service provider and the service consumer) interact and communicate with each other. Examples: In the Request/Response MEP, the service consumer sends a request to the service provider to obtain certain information; the service provider provides the requested information in a dedicated response. In the Publish/Subscribe MEP, the service consumer establishes a subscription with the service provider to obtain certain information; the service provider publishes information (either in regular intervals or upon change) to all subscribed service consumers.
Route Plan	

9 ACRONYMS

Persons producing the Technical Service are invited to provide a list of acronyms as appropriate.

REST

SECOM Secure Communication

10 REFERENCES

IALA Guideline 1128 on Specification of e-Navigation Technical Services

IEC 63173-1 S-421 Route Plan

IEC 63173-2 SECOM

IALA SECOM Service Design Template

11 SERVICE DESIGN DESCRIPTION XML

This appendix contains the formal definition of the service design description.

It is up to the author whether the service design description xml file (which includes the technology dependent definition of the physical data model) is presented in full text or just as an embedded file.