Service Design for VTS Traffic Clearance using SECOM

Contents

[1 Introduction 4](#_Toc151118537)

[1.1 Purpose of the Document 4](#_Toc151118538)

[1.2 Intended Readership 4](#_Toc151118539)

[1.3 Inputs from Other Sources 4](#_Toc151118540)

[2 Service Identification 5](#_Toc151118541)

[3 Technology Introduction 6](#_Toc151118542)

[3.1 General 6](#_Toc151118543)

[3.2 Service Technology and transportation protocol 6](#_Toc151118544)

[3.3 Security 6](#_Toc151118545)

[3.3.1 Communication channel security 6](#_Toc151118546)

[3.3.2 Data Protection 6](#_Toc151118547)

[3.3.3 Data Signature 7](#_Toc151118548)

[3.3.4 Data Encryption 7](#_Toc151118549)

[4 Service Design Overview 8](#_Toc151118550)

[4.1 General 8](#_Toc151118551)

[4.2 Service interfaces 8](#_Toc151118552)

[5 Physical Data Model 11](#_Toc151118553)

[6 Service Interface Behaviour 12](#_Toc151118554)

[7 Service Dynamic Behaviour 13](#_Toc151118555)

[8 References 14](#_Toc151118556)

[9 Acronyms and Terminology 15](#_Toc151118557)

[1.4 Acronyms 15](#_Toc151118558)

[1.5 Terminology 15](#_Toc151118559)

Table of figures

**No table of figures entries found.**

List of tables

N/A

# 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].

## 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 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 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.

## 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.

## 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 IEC 63173-2 SECOM and uses text from the template where valid.

# 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 Technical Design using SECOM |
| Implements | Service Specification for VTS Traffic Clearance 1.0  urn:mrn:iala:techsvc:vts:tcs:1.0 |
| ID | urn:mrn:iala:techsvc:design:vts:tcs:secom  [not official designation, for example only] |
| Version | 0.1 |
| 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 |

# Technology Introduction

## General

This design realizes the service specification [6] using SECOM as defined in [7].

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

## 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).

## Security

### 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 1.1 (RFC-4346)

• 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.

### 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

### 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 and SHA256.

The signature is transported in HEX.

### 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.

# Service Design Overview

## 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.

## 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.

A diagram of a service

Description automatically generated

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.



We will examine the diagram in more detail in 6.

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.

## 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 TODO insert reference.

An XML template for the instance description is provided as an annex to this design. TODO annex reference / definition.

# 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

# 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.

## 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 messageId in the data being passed.

### 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 have an effect on 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.

### Acknowledgement

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

### Subscription

### Remove Subscription

## Signatures

All the envelope signatures must be signed by the Traffic Clearance Service or the consumer (vessel device) that it is serving. This may or may not be the same key used to sign the data.

The signatures must be issued by a Maritime Identity Registry as specified in TODO reference to MCP / IALA MIR Spec.

The service must have a method of automatically obtaining new keys and rotating them as specified in TODO reference.

*Architectural elements applicable for this description are:*

* *Service interfaces*
* *Service operations - functions or procedures which enable programmatic communication with a Service via a Service interface.*
* *Parameters - constants or variables passed into or out of a service interface as part of the execution of a service operation.*

*A service may have one or more service interfaces. Each of them shall be described in a separate sub-section. The sub-section title shall contain the service interface name.*

*For each service interface, the purpose, message exchange pattern and architecture of the Interface shall be described.*

*A service interface supports one or several service operations. Each of them shall be described in a separate sub-section. The sub-section title shall contain the name of the operation. Each service operation sub-section shall contain the following information:*

* *Functionality - shall include a textual description of the operation functionality. In most situations, this will be the same as the operation description taken from suitable diagrams or API documentation.*
* *Parameters – shall describe the unambiguous data structure of input and output parameters of the operation (payload) by using suitable diagrams or references to existing standards and explanatory tables as required while avoiding duplication of documentation that already exists in other documents.*

*It is mandatory to provide a clear description of each service operation parameter and the information about which data types defined in the service data model are used by the service operation in its input and output parameters. If such a documentation exists in the referenced standards a reference to it must be provided, but duplication of effort is not required.*

*It is suggested that the service interface design also provides a sample interface documentation of the service in e.g OpenAPI format [5]. And example definition of the service instance XML (see 5.3) should also be provided to avoid duplication of work by implementing parties.*

# Service Dynamic Behaviour

\*\*\*Draft, following list is an example use case from SECOM, to be adapted to this case\*\*\*

1. The ship wants assistance and searches for an appropriate service in the service registry similar to the use case described in B.2.5.
2. 2)  The ship checks the supported SECOM interfaces of the discovered service by calling the service capability endpoint, see 5.7.13 .
3. 3)  The ship prepares a S-421 Route Plan together with metadata for an UploadObject, see Table 16.
4. 4)  The S-421 is signed and the signature is added to the SECOM\_ServiceExchangeMetadata part of the UploadObject.
5. 5)  ~~The ship nominates the enhanced monitoring service and adds the service to its list of subscribers in order to provide possible route plan updates enroute. The service is added to the ship’s whitelist.~~
6. 6)  The ship sends (uploading, pushing) the S-421 Route Plan to the enhanced monitoring service.
7. 7)  The VTS verifies the signature and the certificate and hence authenticates the sender (the ship) and the route message’s integrity.
8. 8)  The VTS checks the route against local conditions and either confirms the original route plan or makes a new proposed one. If the latter, the enhanced monitoring service makes a proposal and sends (uploads) the proposed S-421 Route Plan to the ship and requests an operational acknowledgement (see 5.7.4) when delivered to the ship and processed by an operator on the ship.
9. 9)  ~~The ship receives the proposed S-421 Route Plan and sends an operational acknowledgment when the officer on watch opens the message.~~
10. ~~10)  When the voyage is ended, the enhanced monitoring service is removed from the list of subscribers and a subscription notification message is sent.~~

\*\*\*TODO describe how interaction between S-421 route service and TCS work\*\*\*

*This section describes the interactive behaviour between service interfaces (interaction specification) and, if required, between different services (orchestration or choreography).*

*The following types of views and (UML) diagrams can be used to describe the dynamic behaviour:*

* *Sequence diagrams*
* *Interaction diagrams*
* *State machine diagrams*

*This section is especially relevant to extend the service design structure (see section 4) from a logical description of interactions to a structure where actual operations and interfaces are referenced. This will also allow better understanding of the interaction between different services.*

# References

| Nr. |  | Reference |
| --- | --- | --- |
| 1. IALA Guideline G1128 |  | THE SPECIFICATION OF E-NAVIGATION TECHNICAL SERVICES |
| 1. IMO FAL.5 /Circ.52 |  | Guidelines for Harmonized Communication and Electronic Exchange of Operational Data for Port Calls |
| 1. IALA Recommendation R1023 |  | MARITIME RESOURCE NAMES |
| 1. IHO Standard S-100 | 5.2.0 | IHO Universal Hydrographic Data Model  <https://iho.int/uploads/user/pubs/standards/s-100/S-100_5.0.0_Final_Clean_Web.pdf> |
| 1. IALA data model S-212 |  | IALA VTS Digital Information Service Product Specification |
| 1. Service Specification for VTS Traffic Clearance | 1.0 | IALA VTS Digital Service Specification |
| 1. IEC 63173-2 SECOM | 1.0.0 |  |
| 1. Service Design – Template SECOM REST |  | G1128 based template for service designs using SECOM REST |
| 1. NIST Digital Signature Standard (DSS–FIPS Publication 186) |  |  |

# Acronyms and Terminology

## 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 |

## 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. |