GUIDELINE

G1191
MARITIME SERVICE REGISTRY (MSR) TECHNICAL SPECIFICATION

Edition 1.2
June 2026

urn:mrn:iala:pub:g1191:ed1.2

International Organization for Marine Aids to Navigation
www.iala.int

DOCUMENT REVISION

Revisions to this document are to be noted in the table prior to the issue of a revised document. The latest edition of the Guideline is the only version in force unless the Guideline is explicitly revoked by the Council.

Date	Revision details	Approval
June 2025	Edition 1.0	Council 02
December 2025	Edition 1.1 • adjusting the usage of callback URL and Transactions IDs during communication with an MSR; • MSR stays connected during communication; • changed the uptime requirement of an MSR from 99.9% to 99.5% of time; • change the cardinality of search retrievals for Searching MSR from 0..1 to 0..n; replace parameter name searchParameter by SearchFilterObject	Council 03
June 2026	Edition 1.2 • Editorial changes • Clarifications of which interfaces are SECOM compatible and which are specific to G1191. • Updates to interfaces to comply with IEC 63173-2. • Refer to IEC 63173-2 (SECOM) rather than specifying an identical interface in this document • Added Annex C that describes multiple MCP use cases	Council 04

CONTENTS

CONTENTS

CONTENTS

CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

1.1. SCOPE

This document aims to define the requirements for implementing a Maritime Service Registry (MSR) that is a part of the Maritime Connectivity Platform (MCP). It is intended primarily for Members, Marine Aids to Navigation (Aton) authorities, international organizations and other appropriate stakeholders that are interested in implementing their own MSR and providing an MSR to allow for service registration and discovery, and secondarily for organizations implementing software systems that make use of an MSR to:

a Register their own service in an MSR and update its information as necessary; and/or

b Find instances of services that fulfil the system user's needs.

The requirement for maritime service registries is based on the *Guideline G1128 Specification of e-Navigation Technical Services* [1] and *Secure communication between ship and shore (SECOM)* [5].

1.2. RATIONALE

In *IMO Resolution MSC.467(101) Guidance on the definition and harmonization of the format and structure of maritime services in the context of e-navigation*, the IMO defines Maritime Services and Technical Services in the context of e-navigation. In the Resolution, the Maritime Services are at the highest level, describing a service in an entirely non-technical manner. One or more Technical Services are associated with a Maritime Service, and these Technical Services are the ones defining the actual information exchange needed to take place to implement a Maritime Service.

Maritime Service Registry (MSR) is a registry of the implementations of Technical Services and is a reference point for information on registered services, and offers discoverability for the registered services. It can be seen as a sophisticated yellow pages phone book. A registry can be searched using several different criteria, including coverage area. MSRs conforming to these requirements will be able to federate searches to the global network of MSR to allow service discovery over a wider network. The MSR is one of the core components of the MCP.

The Technical Services in the Resolution are also defined on three levels, following the same structure as G1128, where MSR supervises all service providers to describe their service in the format of G1128.

1.3. PURPOSE

The main tasks of an MSR are registration of services by the service provider and a discovery service for registered services, so any service consumer can identify available services and find the endpoint of the service. MSR registration needs to be able to register all relevant e-Navigation and e-Maritime services, commercial and non-commercial, authorized and non-authorized, for free and against payment. Each provider of an MSR has their own criteria for acceptance of services to be listed. This Guideline does not impose requirements on providers regarding their criteria. MSR needs to allow service consumers to discover available services and enable the use of the services through given endpoints. To allow for service discovery by clients without the hardcoded knowledge of all existing MSRs, the service registries have a mechanism for implementing a global search that will delegate a search for services to all the MSRs in the network.

MSR is an implementation of the service management concept, which was given in the G1128 specification.

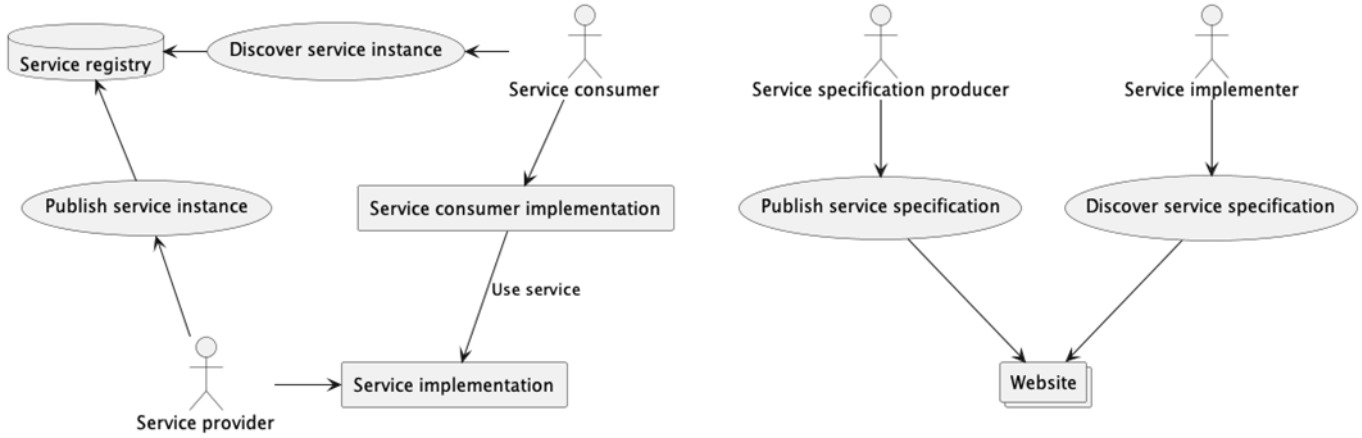

Figure 1 *Service management concept as defined in G1128*

1.4. INTENDED READERSHIP

This service specification is primarily intended to be read by architects, system engineers, and developers in charge of developing and operating an MSR instance. Furthermore, this service specification is intended to be read by enterprise architects, service architects, information architects, system engineers, and developers in pursuing architecting, design, and development activities of related maritime services and consumer applications of these services.

1.5. INPUTS FROM OTHER SOURCES

The service management concept from the G1128 specification was given and implemented throughout previous projects such as EfficienSea2 and Sea Traffic Management. The experiences from these projects have also influenced the service discovery interface defined in SECOM [5][7] that has been adapted as a basis for the interface specification in this document.

1.6. DEFINITIONS OF TERMS USED IN THIS DOCUMENT

The terms “must”, “require”, “must not”, “should”, “recommended”, and ”should not” may follow the definitions as included below for the specific purpose of this Guideline.

- “Consumer” is used to define any consumer calling the MSR via an API to execute a search.
- “Must”, “require”, or “shall” mean that the definition is an absolute requirement of the specification.
- “Must not” or the phrase “shall not” mean that the definition is an absolute prohibition of the specification.
- “Should” or the adjective “recommended” mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- “Should not” or the phrase “not recommended” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.

2. USE CASES FOR MARITIME SERVICE REGISTRIES

To understand the rationale behind the design choices that have guided the development of the requirements listed in this Guideline, the primary use cases of maritime service registries must be outlined and understood. The following use cases have served as the basis for the decisions made and are based on the experiences of previous projects and knowledge of ongoing efforts in defining and implementing Maritime Services. These use cases are not a comprehensive list but are identified as the most important use cases that have been identified.

In terms of an MRN space [2], the MCP domain is defined as the prefix that is used in all MRN issued by that MCP provider. For example, in the MRN urn:mrn:mcp:entity:duckville:donald-duck, the prefix urn:mrn:mcp:entity is a required constant part of each MCP MRN, and the string duckville identifies the domain. The MCP domain corresponds to the IPID string defined in section 4.1 of G1183 [4]. In this context, the MCP domain is defined as all the components, services, users, etc, included in a single MCP instance with an MRN starting with the same prefix.

To reduce unnecessary duplication, the following actor definitions will be used in the following use cases:

- **User** is the human using the consumer information system.
- **Consumer** (ship, shore-based, or other) information system.
- **Maritime service registry** (MSR) of the consumer's MCP domain or other MCP domains.
- **Maritime identity registry** (MIR) of the consumer's MCP domain or other MCP domains.
- **Global MCP Search Platform** (GMSP) facilitates the search for services across multiple MCP domains using a dedicated MMS network.
- **Maritime technical services** (such as for Navigational Warnings, AtoN information) in multiple MCP domains.
- **The maritime service provider** (MSP) provides maritime technical services.

The following diagram shows a high-level view of the general use cases in the MCP domain. The use cases are described in more detail below.

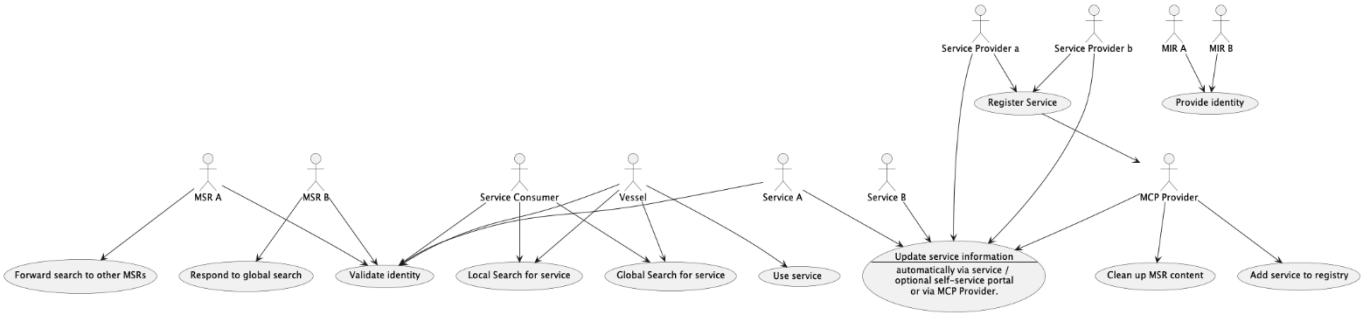

Figure 2 *High-level use cases of MSR*

Sections should be typed continuously, and generally, page breaks or section breaks should not be entered between main sections. It may be necessary sometimes to insert a page break to allow for aesthetic layout, e.g., not breaking a list over two pages.

2.1. USE CASE 1: LOCAL SEARCH

- Who: A consumer registered with a legitimate MCP instance.
- Wants to: Perform a search for a service located in the same MCP domain.
- So that: The consumer can obtain the information required e.g. for planning a route.

2.1.1. DESCRIPTION

A consumer is a registered user of a legitimate MCP instance. They intend to make a trip towards the destination and will need to obtain the information required for planning a route, e.g. navigational warnings or AtoN information. To find the appropriate services that can provide that information, the consumer performs a search query to their respective MSR, submitting as query parameters their:

- route path or other geometry
- the service design MRN (see G1128 [1]) and versions which are compatible with their onboard equipment
- status is “Released”

For example, searching for Traffic Clearance Using SECOM would use the MRN urn:mrn:iala:techsvc:sd:vts:tcs:secom:1.x in the design Id parameter, where the prefix without the version number defines the technical service design and the version number suffix is used to pass a semantic version [3] that is supported to define allowed versions (see https://docs.npmjs.com/about-semantic-versioning#using-semantic-versioning-to-specify-update-types-your-package-can-accept). Thus, version number 1.x would search for all services that implement version 1.0 or higher but less than 2.0 of the design.

2.1.2. ACTORS

- Consumer (ECDIS, Route-Planning System, or human mariner).
- MSR of the consumer's MCP domain.
- Maritime Technical Service, such as: for Navigational Warnings, AtoN information.

2.1.3. FREQUENCY OF USE

Typically triggered when the consumer is planning for a trip in proximity to their base of operations.

2.1.4. PRE-CONDITIONS

- The consumer is registered with a legitimate MCP instance.
- The consumer's MCP instance already includes in its domain at least one service that meets the consumer's requirements.
- The consumer maintains connectivity throughout the whole operation.
- All actors support the SECOM searchService interface.

2.1.5. ORDINARY SEQUENCE

1 User sends a search request to the MSR specifying that this is a local search only, including its route path and other criteria.

2 The consumer's MSR searches its internal database and responds directly to the consumer with a list of the currently registered services that meet the provided criteria. A transaction ID is provided in the response to facilitate audit logging, but the end user must not expect any further responses.

3 The consumer will receive the service information list, which includes the endpoint information.

4 The consumer will make a selection on which of the services it will contact.

5 The consumer will contact the selected maritime information service.

6 The data is rendered and displayed to the user.

7 Post Conditions

The correct maritime information is received by the consumer.

2.2. USE CASE 2: GLOBAL SEARCH

- Who: Consumer: any maritime information system
- Wants to: Perform a search for a service
- So that: The consumer can obtain the information required e.g. for planning a route

2.2.1. DESCRIPTION

The user of the information system intends to make a trip towards a destination and will need maritime information (such as Navigational Warnings, AtoN information) regarding their pre-selected route. To find the appropriate services that can provide that information, the consumer performs a search query to their respective MSR with the same parameters as specified in use case 1.

The user should not need to select whether a local or global search is performed, and the information systems used should perform a global search if required by the nature of the trip and available information in the local MSR.

2.2.2. ACTORS

- User using the consumer information system
- Consumer (ECDIS, Route-Planning System, or other information system
- MSR of the consumer's MCP domain
- Global MCP Search Platform
- MSR Service from another MSR Service Provider
- Maritime Technical Service (such as for Navigational Warnings, AtoN information) in different MCP domains

2.2.3. FREQUENCY OF USE

Typically triggered when the consumer is planning for a trip far away from their base of operations.

2.2.4. PRE-CONDITIONS

- The consumer is registered with a legitimate MCP instance.
- The consumer's MCP instance is interconnected with a compatible instance that includes a service that meets the consumer's requirements in its domain.
- All actors support the SECOM searchService interface.
- The consumer of the search has the ability to poll the MSR for further results.

2.2.5. ORDINARY SEQUENCE

1 User sends a search request to the MSR, including its route path and other criteria.

2 The consumer's MSR searches its internal database and finds a matching registered entry.

3 The consumer's MSR will reply with the local search result and supply a transaction ID that is used when returning results from the other MSRs.

4 The consumer's MSR propagates the search request (along with the geometry provided description of the route) to the Global MCP Search Platform.

5 The Global MCP Search Platform will forward the search for other interconnected MSRs, which might have services that meet the requirements specified in the received request. The forwarded search must follow the structure defined in 4.4.1.1.

6 The other MSRs will respond with the search results from their internal databases. If a search via the search platform does not produce any results, the other MSRs should not respond with an empty result.

7 The consumer's MSR will collect all valid responses identified by the transaction ID and compile a single list of search response entries.

8 The consumer will receive the service information list by polling the MSR to get the results as they arrive via global search. If no results are received, an empty list is returned.

9 The consumer will select which of the services it will contact.

10 The consumer will contact the selected maritime technical service.

11 The data is rendered and displayed to the user.

Note on returned data: The interface will return the service data by default as a subset of the full list of instance metadata defined in G1128 in JSON format as specified by SECOM. By default, no certificate information is returned. However, depending on search parameters, either the thumbprints of full certificate chains or the full certificate chains may be returned.

2.2.6. POST-CONDITIONS

The correct maritime information is received by the consumer.

2.3. USE CASE 3: GLOBAL MARITIME SEARCH PLATFORM (GMSP)

- Who: An MSR that has received a global search from an end user
- Wants to: forward the search to other MSRs
- So that: they can return a list of available services that fulfil the search criteria

2.3.1. DESCRIPTION

An MSR receives a search from an end user that must be forwarded to other MSRs to perform a global search. The search is defined in use case 1, and the actual search parameters, with the exception of the geometry, are not of interest from the perspective of this use case.

2.3.2. ACTORS

- Consumer (ECDIS, Route-Planning System or human mariner)
- MSR Service of the consumer's MCP domain MSR
- The MMS network provides the GMSP
- Other MSRs participating in the GMSP (MSRa, MSRb, etc.)

2.3.3. FREQUENCY OF USE

Triggered whenever a user executes a global search against any compliant MSR.

2.3.4. PRE-CONDITIONS

- The MSR is a participant in the GMSP
- The MSR knows the subjects defined in the GMSP
- The MSR always maintains connectivity
- All actors support the GMSP

2.3.5. ORDINARY SEQUENCE

1 The MSR receives a search from the consumer.

2 The MSR generates a transaction ID, which is a UUID-v4.

3 The MSR executes the search against its own database and returns the result, including the generated transaction ID.

4 The MSR uses its internal mapping of the GMSP subject list to define which subjects the search needs to be published to, according to the geometry of the search. For the sake of example, the subjects applicable to the search are subject A and subject B.

5 The MSR adds the endpoint for uploading results to the search published in all of the relevant subjects in GMSP (subject A, subject B).

6 MSR A is subscribed to subject A; MSR B to subject C; and MSR C to subject B and subject A, and MSR D to subject B. MSR B does not see the search and does nothing.

7 MSR A executes the search in its own database and uploads the results to the endpoint provided in the search message.

8 MSR C executes the search in its own database and uploads the results to the endpoint provided in the search message.

9 MSR D executes the search in its own database and gets no result, thus not responding in any way.

10 The MSR collates the responses from both MSR A and MSR C and returns the collated information in the subsequent requests from the consumer that are identified with the transaction ID.

2.3.6. POST-CONDITIONS

The correct list of services is received by the consumer.

2.4. USE CASE 4: SERVER IMPLEMENTATION OF GLOBAL SEARCH

- Who: Consumer: any MSR instance
- Wants to: Perform a global search for a service
- So that: They can return search results from other MSRs

2.4.1. DESCRIPTION

An MSR instance has received a search for a service that needs to be delegated to the global search platform in order to return results from multiple MSRs.

There are several variations of this use case depending on the search parameters and the requirements of individual MCP domains.

- Search with geometry
- Search without geometry
- MSR requiring authentication to return results with or without geometry

All three of these variations will be described as subsets of the same use case.

All other search parameters are irrelevant from the perspective of this use case.

These three variants are suitable for use cases 1 and 2 but have been left out of those descriptions for simplicity and are described here, where the use case is more technical in nature.

2.4.2. ACTORS

- A consumer who executes a global search on MSR A.
- The MSR that the consumer is using to perform the search (MSR A in the following descriptions).
- MMS network provides the global search platform. This is separate from the default MMS network, and access is restricted to vetted MSRs.
- MSRs responding to a search received via the MMS network (MSRs X, Y and Z in the following descriptions).

2.4.3. FREQUENCY OF USE

Triggered every time a global search is executed.

2.4.4. PRE-CONDITIONING FOR ALL VARIATIONS

- MSR receives a global search from a consumer.
- Multiple MSRs are a part of the MMS network, providing the global search platform.

2.4.5. ADDITIONAL PRE-CONDITION FOR VARIATION 3

The consumer has provided a certificate proving its identity.

2.4.6. ORDINARY SEQUENCE

1 A consumer sends a search to MSR A.

2 MSR A checks for the existence of a certificate in the incoming request, depending on the MCP domain requirements.

   a The certificate is ignored, and no validity is checked.

   b The certificate is ignored, and no validity is checked.

   c If MSR A limits its use and requires authentication, it will check the validity of the incoming certificate at this point. If the certificate is invalid, the MSR will return an error to the consumer.

3 MSR A decides if authentication is required, e.g. based on the search parameters.

4 If authentication and authorisation are required, authentication is done. If the consumer is not authenticated or authorised, the next step will not be executed, and an error is returned to the consumer. MSR A executes the search in its local database.

5 MSR A generates a transaction ID for the search.

6 MSR A returns the local search result and the transaction ID to allow the consumer to track incoming results to this search.

7 MSR A selects the MMS subjects to which the search will be published:

   a Without a geometry, the search is published to the global MMS search subject that all participating MSRs must be listening to.

   b The geometry is mapped to the predefined set of search subjects based on geometry, and those subjects that cover the area in the geometry are used to publish the search to.

   c As above, depending on the search parameters.

8 The forwarded search will include the provided certificate that will be forwarded to all participants. The generated transaction ID is used to generate the endpoint to which results must be returned. Uploading results to this endpoint allows collation of search results.

9 The MMS network pushes the search in all valid topics to all listening MSRs

10 Depending on variation:

   a All MSRs X, Y and Z receive the search.

   b Only MSRs X and Z receive the search as they are the only ones interested in the defined search subjects.

   c As above, depending on search parameters.

11 If any of the participating MSRs requires authentication, the authentication is performed. If the consumer is not authenticated, no results are returned, and no error is returned.

12 All MSRs that received the search should execute it in their local database.

13 The results of the search should be returned via API call from MSRs X, Y, and Z to MSR A.

14 MSR A must collate the results returned and return them to the consumer in a subsequent call to the search that is identified with the transaction ID of the search.

15 After a predefined timeout, MSR A may begin to ignore any further responses to the search.

Note on returned data: The interface returns the service data by default as a subset of the full list of instance metadata defined in G1128 in JSON format as specified by SECOM. The certificates of the services are not returned.

2.4.7. POST-CONDITIONS

The correct maritime information is received by the consumer.

2.5. USE CASE 5: VALIDATE IDENTITY

- Who: An MSR.
- Wants to: Validate the identity of a consumer (service, ship system, etc).
- So that: It can authenticate the source of the request and decide if the requested action is authorized.

2.5.1. DESCRIPTION

An MSR has received a request (search, update, etc.) and it wants to validate the identity of the consumer sending the request. Note that, depending on the request, this use case is either mandatory or optional.

2.5.2. ACTORS

- The consumer who is the source of the request
- An MSR that receives the request
- A MIR that has provided the identity of the consumer

2.5.3. FREQUENCY OF USE

Frequent – at most every time an MSR receives a request but may be less.

2.5.4. PRE-CONDITIONS FOR ALL VARIATIONS

- The consumer provides a certificate in the request.
- The consumer has made a request to the MSR.

2.5.5. ORDINARY SEQUENCE

- Consumer requests the MSR.
- The MSR validates the certificate and signature of the request by following the procedure described in section 5 of G1183 [4]. MSR may contact the issuing MIR for extra verification if desired.
- The MSR decides how to respond based on the results of the consumer's identity.

2.5.6. POST-CONDITIONS

The MSR has ensured that the identity provided is valid.

2.6. USE CASE 6: REGISTER SERVICE

- Who: A maritime service provider who provides a maritime service
- Wants to: Register their service for listing in an MSR
- So that: The service is discoverable to consumers

2.6.1. DESCRIPTION

A maritime service provider wants to register their new service in their MSR. By registering, it means the process of ensuring all necessary information for the addition of a service to the MSR is present before actually adding it to the MSR.

2.6.2. ACTORS

- A maritime service provider
- An MSR provider

2.6.3. FREQUENCY OF USE

Rarely, only when new services need to be added to the MSR.

2.6.4. PRE-CONDITIONS FOR ALL VARIATIONS

The maritime service provider is already registered with the MSR provider and can obtain a valid identity for the service from the MIR.

2.6.5. ORDINARY SEQUENCE

- The service provider obtains an identity for the service instance from the MIR.
- The service provider has created the instance XML document and has the public certificates available.
- If the MCP provider provides a self-service portal that allows the service provider to add their service to the MSR, go directly to use case 7B.
- The MCP provider has a documented process on the steps needed from a service provider to enable the addition of the service into the registry. The process depends on each provider and is not in the scope of this guideline.

2.6.6. POST-CONDITIONS

The MCP provider has enough information to add the service to the service registry and enable updating of service metadata according to all variants of use case 8.

2.7. USE CASE 7A: ADD SERVICE TO REGISTRY

- Who: An authorised user of the MCP provider
- Wants to: Add a new service to MSR
- So that: The service is discoverable

2.7.1. DESCRIPTION

The MCP provider does not provide a self-service method for authorised users to add new services to the registry. The addition of each new service must thus be done by the MCP provider based on information obtained in use case 6.

2.7.2. ACTORS

- MCP provider personnel
- MSR of the MCP provider

2.7.3. FREQUENCY OF USE

Rarely, only when new services need to be added to the MSR.

2.7.4. PRE-CONDITIONS

The MCP provider has all the necessary information on the service available: current certificates and instance description XML according to G1128 [1]. The service should be up and running before this use case is undertaken.

2.7.5. ORDINARY SEQUENCE

- MCP provider personnel access internal tools to add a new service to the registry with the instance description and a valid certificate.
- MSR validates the certificate.
- MSR validates the instance description.
- MSR tests the polling interface of the service. If unsuccessful, the service is marked as disabled, and an error is shown to the user.
- MSR verifies that the certificate provided during service addition matches the certificate provided by the service. If unsuccessful, the service is marked as disabled, and an error is shown to the user.
- An instance is added to MSR and is immediately discoverable if it responded correctly to the tests above.
- If the tests above fail, the MSR must provide a method for the user to be able to update information or force a retest. Once tests in steps 4 and 5 are successful, the service is marked as enabled and is discoverable.

2.7.6. POST-CONDITIONS

Service is listed in MSR and is discoverable.

2.8. USE CASE 7B: ADD SERVICE TO REGISTRY

- Who: An authorized user of the maritime service provider
- Wants to: Add a new service to MSR
- So that: The service is discoverable

2.8.1. DESCRIPTION

The MSP uses the information collected in use case 6 to add the service to the registry in a self-service functionality (e.g. portal) offered by the MCP provider.

2.8.2. ACTORS

- MSP
- MCP provider self-service service
- MSR

2.8.3. FREQUENCY OF USE

Rarely, only when new services need to be added to the MSR.

2.8.4. PRE-CONDITIONS

The MCP provider has provided a self-service portal that allows authorized users to add new services to the MSR. The generation and provision of the certificate for the service may be a part of the service addition or a separate step. The user must have all of the information necessary for the instance description available.

2.8.5. ORDINARY SEQUENCE

1 The service provider user accesses the self-service portal of the MCP provider.

2 The user begins the service addition

3 The user enters the instance description information

4 If the portal allows for the generation of service certificates during addition, the certificates will be generated and available for delivery to the user. If the generation of certificates is not allowed, the user must upload the public certificate of the service.

5 The process is paused until the service is up and running with the correct certificates.

6 The MSR will run the tests in steps 4 and 5 in use case 7A.

7 If all tests are successful, the service is marked as enabled and is discoverable. If not, the user must take steps to correct issues and continue from step 6.

2.8.6. POST-CONDITIONS

Service is listed in MSR and is discoverable.

2.9. USE CASE 8A: UPDATE SERVICE AUTOMATICALLY

- Who: A maritime service
- Wants to: Update its metadata in the MSR
- So that: The service information is up to date

2.9.1. DESCRIPTION

The maritime service must update its certificate information every time it has a new certificate issued. Also, during the deployment of a new version of the service instance, the metadata of the service may need updating. This includes, but is not limited to, the instance version number. At least the version number of the instance and the certificate must be updatable via automatic means.

2.9.2. ACTORS

- The maritime service
- MSR

2.9.3. FREQUENCY OF USE

At least once a month per service. Due to monthly certificate changes.

2.9.4. PRE-CONDITIONS

The service is registered and added to the MSR and has a valid certificate stored in the MSR.

2.9.5. ORDINARY SEQUENCE

1 An action requiring the update of service metadata in MSR takes place, e.g. service receives a new certificate from MIR or is deployed with a new version.

2 Service generates an update request and signs it using a certificate that the MSR has stored.

3 Service obtains a one-time encryption key from the MSR.

4 Service encrypts the update request and signature.

5 An encrypted message is sent to MSR.

6 MSR decrypts the message.

7 MSR verifies the update request against the certificate it has in store.

8 MSR verifies that only changes that are allowed in the service information are present in the update request.

9 If the update request is valid, MSR updates the service information.

2.9.6. POST-CONDITIONS

The service information in the MSR has been updated.

2.10. USE CASE 8B: UPDATE SERVICE VIA SELF-SERVICE

- Who: A maritime service provider.
- Wants to: Update the metadata of its service in the MSR via a self-service portal.
- So that: The service information is up to date.

2.10.1. DESCRIPTION

Some of the metadata of the service may be outside the scope of what can be automatically updated by the service but is allowed to be updated by the MSP in a self-service tool.

2.10.2. ACTORS

- MSP
- MCP provider self-service tool
- MSR
- Optionally, the MCP provider personnel

2.10.3. FREQUENCY OF USE

Depending on need, but rare in most cases.

2.10.4. PRE-CONDITIONS

MCP provides a self-service method of updating service information for authorized users, and the MSP user has all the necessary data available. The version number of the instance and the certificate of the instance must be updatable automatically.

2.10.5. ORDINARY SEQUENCE

1 An action requiring the update of service metadata in MSR takes place that cannot be done automatically, either due to MCP provider policies or limitations in this guideline.

2 The necessary data is collected by MSP.

3 MSP uses the self-service tool to update the information.

4 If desired, the MCP provider can review the changes before approval.

2.10.6. POST-CONDITIONS

The service information in the MSR has been updated.

2.11. USE CASE 8C: UPDATE SERVICE VIA MCP PROVIDER

- Who: A maritime service provider.
- Wants to: Update the metadata of its service in the MSR by contacting the MCP provider.
- So that: The service information is up to date.

2.11.1. DESCRIPTION

Some of the metadata of the service may be outside the scope of what can be automatically updated by the service or via an optional self-service tool by the MSP, and requires a change by the MCP provider.

2.11.2. ACTORS

- MSP
- MCP provider
- MSR

2.11.3. FREQUENCY OF USE

Depending on need, but rare in most cases.

2.11.4. PRE-CONDITIONS

An update to service information is required, and that cannot be done automatically or through an optional self-service tool provided by the MCP provider to the MSP.

2.11.5. ORDINARY SEQUENCE

1 An action requiring the update of service metadata in MSR takes place that cannot be done automatically, either due to MCP provider policies or limitations in this guideline.

2 The necessary data is collected by MSP.

3 MSP delivers the necessary information to the MCP provider according to an agreed process.

4 MCP provider validates the information.

5 MCP provider uses internal tools to update the service information.

2.11.6. POST-CONDITIONS

The service information in the MSR has been updated.

2.12. USE CASE 9: REMOVE SERVICE

- Who: A maritime service owner.
- Wants to: Remove service information from the registry.
- So that: The MSR provides accurate information.

2.12.1. DESCRIPTION

If a service instance is no longer available or a ship system or any other system registered in the service registry for discoverability should no longer be available, a process needs to be in place to enable the removal of the information from the service registry.

2.12.2. ACTORS

- Service provider or ship system
- MCP provider
- MSR

2.12.3. FREQUENCY OF USE

Infrequent for maritime services. For systems that are mainly consumers of services but need to register for discoverability, the need may be more frequent depending on the findability in global search.

2.12.4. PRE-CONDITIONS FOR ALL VARIATIONS

Service is registered in MSR. Ship systems are identified by having an MMSI and optionally an IMO number as part of the service information.

2.12.5. Ordinary Sequence for Service Providers

1 The service provider contacts the MCP provider via an agreed-upon method to remove service from the MSR.

2 The MCP provider validates the request (exact process depends on the provider).

3 The MCP provider sets the status of the service to “deleted”.

4 MSR no longer returns the service in search results.

5 After a grace period of 14 days, the service is removed from the registry automatically.

2.12.6. Ordinary Sequence for Ship Systems

1 Ship systems submit an automated request for the ship system removal from the MSR to the MSR.

2 MSR notifies the MCP provider of the removal request.

3 The MCP provider validates the request (exact process depends on the provider).

4 The MCP provider sets the status of the service to “deleted”.

5 MSR no longer returns the service in search results.

2.12.7. Post-Conditions

Service is no longer discoverable via MSR.

2.13. USE CASE 10: CLEAN UP REGISTRY CONTENT

- Who: An MCP provider.
- Wants to: Ensure that all MSR listings are up to date and valid.
- So that: The MSR provides accurate information.

2.13.1. Description

While the previous use case describes an ideal scenario where providers of services or ship systems proactively ensure that obsolete or defunct entries are removed from the MSR, it is more than likely that MSRs will require regular checking and clean-up of the entries in the registry. This is an important process to ensure that MSRs returns results that are fit for purpose.

2.13.2. Actors

- MCP provider
- MSR

2.13.3. Frequency of Use

Regularly, for example, once a month.

2.13.4. Pre-Conditions

The MCP provider has an established process and requirements for services to stay active and discoverable in the MSR that have been communicated to all entities that have registered entries in the MSR.

2.13.5. Ordinary Sequence

1 Scheduler triggers a regular check in the MSR.

2 MSR goes through each entry and flags those that fulfil the pre-defined criteria of an entry to become a candidate for removal.

3 MSR notifies the MCP provider of the resulting list of entries.

4 MCP provider goes through each entry, removing those that it deems necessary.

2.13.6. POST-CONDITIONS

Obsolete or defunct entries are removed from MSR, and search results return services that are available and fit for purpose.

3. REQUIREMENTS

3.1. FUNCTIONAL REQUIREMENTS

1 MSR must allow consumers to search for services via an API call

The attached Open API template for MSR implementations provides a formal listing of all API endpoints and the input and output data for each endpoint, see Annex A.

- The search interface must be compatible with the SECOM searchService interface [5]. While the interface must be compatible with the searchService interface defined by SECOM, not all of the parameters defined in SECOM are required. The required parameters and how they work are based on the work done to identify how systems will use the API interface to search for services, and are not based on the needs of a human user to be able to search for services without knowing exactly what functional needs the service must be able to fulfil. The searchService must support HTTP POST requests with all parameters in the body. In this case, the HTTP header X-Http-Method-Override with the value GET should be passed. The path to the searchService interface in REST implementations must be /v2/searchService. The searchService must support HTTP GET with query parameters in the query string. The use of multiple parameters in a single call joins the parameters with an AND statement. OR searches are not supported. Consumers must call searchService multiple times and combine the results to achieve an OR search. A searchService call without any parameters should not be implemented in consumers. MSR must not consider a search without any parameters as a global search and must treat it as if localOnly=true was passed.
- The interface must accept the following SECOM SearchParameters in the query attribute of the EnvelopeSearchFilterObject:
  - The interface must accept the following SECOM SearchParameters in the query attribute of the EnvelopeSearchFilterObject:
  - designId (MRN) – the MRN of the service design that the service implements.
  - mmsi (CharacterString) – the 9-digit MMSI number of the vessel being searched for. This parameter must be used in conjunction with the designId parameter to prevent misuse. If present without the designId parameter, an error with HTTP status code 400 must be returned.
  - imo (CharacterString) – the 7-digit IMO number of the vessel being searched for. This parameter must be used in conjunction with the designId parameter to prevent misuse. If present without the designId parameter, an error with HTTP status code 400 must be returned.
  - instanceId (MRN) – the MRN of the service instance. This maps to the id-element in the G1128 conformant XML metadata. The version suffix may be omitted, and every available version of the instance will be returned.
  - status (ServiceInstanceStatus) – used to ensure, from a consumer point of view, that in most cases, only released services are returned. If the parameter is not passed, MSR must default to the value “released”.
- The interface must accept the following parameters in the EnvelopeSearchFilterObject:
  - geometry (CharacterString) – geometry of service coverage area in WKT format. Results must include all services for which the coverage area intersects with the geometry and all services without a coverage area defined (i.e. global services).

- localOnly (boolean) – used to tell MSR if the search is intended to be local. If not present or unset with a valid boolean value, “false” is used as the default and a global search is performed.

- The interface may accept the following SECOM SearchParameters in the query attribute of the EnvelopeSearchFilterObject:
  - name (CharacterString) – the name of the instance.
  - version (CharacterString) – version number of the instance. Should follow semantic versioning.
  - keywords (Array of CharacterString) – CharacterString array of keywords.
  - description (CharacterString) – human-readable description of the instance.
  - dataProductType (Array of CharacterString) – the S-100 or other data products that is supported by the service.
  - specificationId (MRN) – the MRN of the service specification that the instance implements.
  - serviceType (MaritimeServiceType) – one of MS[1-16] or Other as defined in SECOM [5]. This refers to the IMO specified classification of high-level types or domains of services.
  - unlocode (CharacterString) – the UN/LOCODE, which may be used as a parameter instead of a geometry.
  - endpointUri (URI) – the URI of the instance endpoint.

  If any of these values are unsupported, but valid values are provided in the search, a result must be returned. If only unsupported parameters were passed, an HTTP status 501 Not Implemented must be returned.
- The return values of the search are: The full list is defined in 4.2.3 with the following requirements set for the returned data.
  - transactionId (UUID) – the UUID given to this transaction. Used to identify subsequent requests from the client when polling for global search results.
  - sourceMSR (MRN) – attached to each entry when data is received via global search. Left empty or unset for localSearch.
- MSR must allow the consumer to specify if the search is intended to be only local or global.
- A local search is defined as searching only the registry of the MSR that receives the request. This is done by using the localOnly parameter defined above. When a global search is performed, the consumer is expected to poll the MSR for responses returned from other MSRs.
- Local search must be a synchronous call.
- Local search must always return the same results if called by the same user, and no changes have occurred in registered services.
- Local search should respond in five (5) seconds or less.
- Global search must be a synchronous local search and polling by the client to retrieve results from other MSRs.
- The polling operation is an HTTP POST request to the URL /v2/retrieveResult/[transactionId]. The HTTP header X-Http-Method-Override with the value GET should be passed
- The polling must be done three (3), six (6) and ten (10) seconds after response to the initial search has been received. If a polling pull receives HTTP 404 it does not indicate that further results are not coming. A minimum of three pulls must be completed as specified.

- The consumer may poll for extra results at any time between 10 and 30 seconds.
- The search transaction must be held open for 30 seconds on the MSR. Any subsequent results from other MSRs or call to retrieveResult may be ignored.
- The MSR must return only new data each time the poll is done. Paging must not be available when polling.
- The first response of global search must never have HTTP status code 404.
- In many cases, the MSR is intended for use only by consumers who must have a valid maritime identity supplied by a MIR, and in those cases, there is no reason for the API not to limit its use to consumers with a maritime identity. However, if the MSR desires, it may be open to receiving searches from systems without a valid maritime identity (e.g., for searches from consumer devices). If a valid maritime identity is not required, the results returned from a global search may be severely limited.
- Vessel endpoint must only be returned to consumers who have provided a valid maritime identity in the search request.
- The service is considered a vessel if the IMO number or MMSI number is present.
- The response of the search must be signed.
- When handling results from global search, the MSR that received the search from the consumer must verify all replies from other MSRs but the results received by the consumer must always be signed by the MSR that received the search.
- MSR must support semantic versioning in version numbers.
- Semantic versioning describes a commonly understood method of declaring version numbers [3]. The only deviation in the maritime specification and design world is that odd-numbered major versions are used to describe documents published for testing, and even numbers for production-ready. Using it allows for permitting wildcards when searching with a version number to prevent the need to explicitly declare all possible version numbers that are acceptable.
- To reuse a previous example, searching for Traffic Clearance Using SECOM would use the MRN urn:mrn:iala:techsvc:sd:vts:tcs:secom:1.x in the designId parameter, where the prefix without the version number defines the technical service design and the version number suffix is used to pass a semantic version that is supported. to define allowed versions. Thus, version number 1.x would search for all services that implement version 1.0 or higher but less than 2.0 of the design.

2 The following fields must be available for each entry in the MSR. See G1128 for the list of fields that must be supported, and refer to the instance schema for further technical details. In addition, the business rules must be taken into account:

- IMO or MMSI number – Must only be present for services that are being registered for vessels to allow for mapping between AIS data and service registry when using MSR to discover endpoints available onboard.
- statusEndpoint – This field must point to the ping interface of the service for all shore-based services. This must be a working URL.
- endpoint – This must be submitted in a way that, depending on the transport, it will work without parsing or cleaning. For example, for SECOM services, it must be defined without the trailing slash (/) so that concatenating the SECOM interface definition paths creates a valid URL without double slashes (//) in the path.

3 MSR must have an audit log of all changes to registry content. The audit log must contain information on what, when, and who made the change. The audit log must be stored for at least one (1) year.

4 MSR must allow changes to registry content only from authenticated users.

5 MSR must enable the MCP provider to maintain registry content.

- MSR must have a method of adding, updating and removing entries from the registry by the MCP provider. This guideline does not mandate the method the MCP provider manages the entries in the registry.
- The MCP provider must not have direct access to edit the registry database without all changes being logged in the audit log.

6 MSR must enable service providers to automatically update the following instance data:

- version
- endpoint
- statusEndpoint
- apiDoc
- certificate

7 MSR may provide an interface for service providers to update service information. The service provider must not edit the following fields:

- id – except for version number suffix
- organizationId – of either the provider or the producer

The editability of any other fields in the service information is up to the MSR provider to allow. This guideline does not place any other requirements on how the service providers may update the service information.

8 MSR may allow service providers to add services to the MSR. The process of how a service provider adds a new service to the registry is not defined in this guideline. It may be via a self-service portal or via a more manual process through the MSR provider. All of the information about the service must be provided by the service provider except for the following:

- id – This is determined by the certificate and depends on the MIR process for providing new identities.
- organizationId – of either the provider or producer, and for the aforementioned reason.

9 Adding vessels to MSR must follow the same process as adding new services to MSR. Vessels should be added to only one MSR that participates in global research if they need to be discoverable. The MSRs they are added to should belong to the same MCP domain that has issued the maritime identity for the vessel. If the vessel has multiple endpoints for different designs that it implements, then multiple entries for the vessel are required in the MSR. Vessel endpoints should be registered only in the MSR of their MCP provider if the MSR participates in global search to allow for discoverability. If the MCP provider of the vessel does not participate in global search, it is allowed for the endpoints to be registered in another MSR that participates in global search. The following information must be present for a vessel added to an MSR: MMSI and/or IMO to allow for mapping between AIS, etc., data and vessel MRN

10 MSR must allow multiple entries from a single ID. The ID must not be used as a primary key, as e.g. vessels may need to have several entries in the MSR in order to have different endpoints for different service designs that they support.

11 ID requirements:

- ID must be a valid and unique MRN for that instance.
- The only requirement for an ID is that it is a valid MRN and globally unique. MCP providers must ensure that a service added to the registry either has a unique ID that is not found in global search, or if results

are returned, they refer to the same instance. This means that an instance may be registered in multiple MSRs.

- ID must not be assumed to have semantic meaning.
- ID must match the certificate MRN.

  All services registered in the MSR must support the ping interface. The call to the ping interface must be done at least once a day. If no response is received, the call must be retried six (6) times every ten (10) minutes or until a response is received. If no response is received, service must be flagged for review. Entries in the registry that have an MMSI and/or IMO number must not be pinged. These entries should not have the statusEndpoint field populated.

12 MSR must check the availability of services regularly. All services registered in the MSR must support the ping interface. The call to the ping interface must be done at least once a day. If no response is received, the call must be retried six (6) times every ten (10) minutes or until a response is received. If no response is received, service must be flagged for review. Entries in the registry that have an MMSI and/or IMO number must not be pinged. These entries should not have the statusEndpoint field populated.

13 MSR should participate in the global search.

14 Global search requires MSR to support MMS [6].

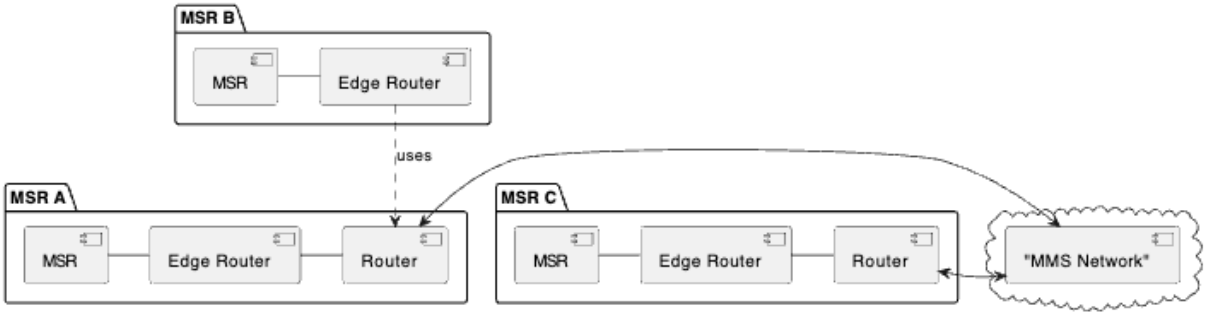

Figure 3 *Functional requirements: MSR supporting MMS*

- An MSR must have a built-in edge router.
- MSR providers should provide their own router or have an agreement with an MSR provider that provides a router to which their edge router connects.
- An MSR must subscribe to the global subject and the relevant search area subjects:
  - urn:mrn:mcp:msr:search:global – The search subject for searches covering the whole globe (i.e., no geometry or default geometry of the whole globe).
  - urn:mrn:mcp:msr:search:searcharea:[i-xxiv] – The search subjects are split by geometry using search areas defined in Annex B.
  - The method for handling the addition or splitting of subjects will be defined in future versions if the need arises.
- Global search results must not be sent via MMS but through the interface defined in 4.4.2.
- Global search is not required to always return the same result.

- For the same consumer, the MSR may return different results in global search when compared to local search. The rationale for this is that there may be services registered in the MSR that the MSR never returns in global search, but may return to the user if they access the MSR directly.
- MSR may have its own rules on what is returned in global search results.
- The MSR that is collating the results of the global search may filter the results returned to the consumer.
- Participants in the global search network must handle their own costs for outgoing data.

3.2. NON-FUNCTIONAL REQUIREMENTS

- Consumer must allow the human end-users to verify the list of services retrieved and selected.
- This means that the human end-user needs to be able to see the search or searches that were submitted, the returned results, and the used services. It is important to keep in mind that the MSR is intended as a technical service registry, and as such, the consumer of an MSR should always be an information system and not a human user. In most cases, requiring a human user to do service selection will increase cognitive load and reduce the utility of the information systems.
- MSR must have measures in place to prevent DDOS attacks.
- This guideline does not specify exactly how the prevention should be done, as it is dependent on the deployment environment. A compliant MSR implementation must be tested against common DDOS attack vectors and have a documented risk assessment and mitigation strategy in place.
- MSR must have measures in place to limit the risk of using MSR to spam services.
- What spamming means depends very much on the service. In most cases, services should be able to prevent malicious spamming attacks with nonsense requests by doing XML schema validations on S-100 messages. It is recommended that any other services published in the MSR that use different data types have a similar mechanism in place.
- Preventing spam attacks on vessel endpoints listed in the MSR is why searching for vessel endpoints must be limited to authenticated consumers.
- Participation in the global search platform requires vetting by the MCP Consortium.
- G1183 describes the role of the MCP Consortium in relation to the MIR. In addition to those tasks, the MCP Consortium will vet all participants in the global search platform and ensure that all parties follow this guideline.
- MCP Consortium endorsement is required for participation in the global search platform.
- MCP Consortium endorsement establishes a base level of trust between MSRs.
- The endorsement establishes that all endorsed MSRs have compatible and trustworthy processes in place to identify entities given a maritime identity and what is required of service providers and their services. However, the endorsement does not imply the need to trust search results or services returned from endorsed MSRs. The MCP Consortium is working on a trust system that may enable more fine-grained delegation of trust apart from the pure authentication that a valid maritime identity provides.
- MSR providers should ensure that MSR returns accurate data.
- The requirement listed above that the MSR must ping all non-vessel services registered and flag them for further checking if they are unavailable is a part of this requirement. The MSR provider must have a procedure in place to vet the availability of services and temporarily or permanently remove them from the MSR search results.
- MSR must have an availability of at least 99,5% during a calendar year.

- The consumer will not receive any information on whether using the service returned will incur costs to the consumer.
- Current information on services has no method of listing service costs.

4. INTERFACE DEFINITIONS

For all the interfaces defined below, only a REST interface is defined. This section is intended primarily as guidance, see Annex A for the normative OpenAPI definition of the interfaces.

4.1. COMMON INFORMATION

4.1.1. HTTP RESPONSE CODES

Unless otherwise specified in specific interfaces, the response codes defined in SECOM [5], Clause 9 apply.

4.1.2. RESPONSE OBJECT

A standard response must always have the following fields: message – a non-empty string that describes the result of the operation. In error situations, it must have a reasonable explanation of the error.

4.2. CONSUMER INTERFACES

The definition of this interface is intended to be compatible with the search service interface defined in SECOM [5]. As such, the list of parameters includes many parameters that are defined as must be ignored as the data model of services does not support those parameters.

4.2.1. OPERATION GET /V2/SEARCHSERVICE

The interface must be compatible with the Search service interface defined in SECOM [5], Clause 9.

4.2.1.1. Request parameters

See 3.1 (The interface must accept the following parameters) for the parameters that an MSR must support in incoming requests, and 3.1 (The interface may accept the following parameters) for parameters that an MSR may support.

4.2.1.2. Service response

See below 4.2.3

4.2.2. OPERATION POST /V2/SEARCHSERVICE

The interface must be compatible with the Search service interface defined in SECOM [5], Clause 9.

4.2.2.1. Request parameters

No request parameters are supported when using the POST operation. If request parameters are passed, the server must respond with an HTTP status code 400.*

4.2.2.2. Request body

See 3.1 (The interface must accept the following parameters) for the parameters that an MSR must support in incoming requests, and 3.1 (The interface may accept the following parameters) for parameters that an MSR may support.

4.2.2.3. Service response

The service response must be compatible with the Information output for search service interface as described in SECOM, Clause 9.2.2 “Data exchange model”.

4.2.3. /V2/SEARCHSERVICE RESPONSE

The service response must be compatible with the Information output for search service interface as described in SECOM, Clause 9.2.2 “Data exchange model”, see the requirements for handling some of the returned data.

4.2.4. OPERATION POST /V2/RETRIEVERESULT

This interface is used by the consumer to retrieve the search results returned from a global search. The URL of the request must include the transaction ID returned in the first response that returned the local results to identify the search for which the retrieval is being done. The interface must be compatible with the Search service interface defined in SECOM [5], Clause 9.

4.2.4.1. Request parameters

See Clause 9 of SECOM.

4.2.4.2. Service response

The service response must be compatible with the Information output for search service interface as described in SECOM, Clause 9.2.2 “Data exchange model”, see the requirements for handling some of the returned data.

4.3. SERVICE INTERFACES

4.3.1. OPERATION PUT /API/G1191/V2/UPDATESERVICE/[INSTANCEID]

The MSR must support automated update of some of the service information to ensure that it has an up-to-date certificate, endpoint, API documentation and version information of the service. This operation fulfils the requirement 6.

4.3.1.1. Request parameters

No parameters are allowed.

4.3.1.2. Request body

The following parameters must be supported:

Table 1 Request body

Attribute	Type	Multiplicity	Definition
certificates	string	0..3	Public certificate x.509 in PEM format. Should include all currently valid certificates of the instance.
version	string	0..1	Version number of the instance. Semantic versioning should be preferred.
endpointUri	URI	0..1	The endpoint of the service. The format and completeness of the endpoint depend on the endpoint type.
apiDoc	URL	0..1	The URL to the documentation of the instance. Preferably not only API documentation but also necessary contact information etc.
statusEndpoint	URL	0..1	The URL to the ping interface of the service. This must be the complete URL that responds.

Any other parameters that the MSR provider allows to be automatically updated must be documented by MSR provider. This guideline does not consider how any other information is handled. The MSR must complete the following checks for input:

- Certificate validity
- Endpoint must be a valid URI
- apiDoc must be available and respond with an HTTP status code 200

- statusEndpoint must be available and respond with an HTTP status code 200 and include a valid timestamp in the response.

4.3.1.3. Service response

HTTP status 200 and message content must be the current timestamp if successful. In case of an error, the adequate HTTP status code must be returned, and the message must contain a clear indication of why the operation failed.

4.4. GLOBAL SEARCH INTERFACES

4.4.1. MMS IMPLEMENTATION

The global search platform is based on MMS for the delegation of searches to the whole network. MMS is defined in RTCM Specification 13900.0 [6]. A compliant MSR must implement the edge router functionality and must have a router available. A compliant MSR should implement a router to participate in the global search network. A compliant MSR edge router or router should not allow any other subjects outside those defined in this guideline. Routers or edge routers are not expected to forward any messages outside of the subjects defined in this guideline. The use of MRN-addressed messages should also be avoided, and routers are not expected to forward MRN-addressed messages.

4.4.1.1. Search message

The search message must be a send message in MMS with the applicationMessage part in the following format, see Annex A for formal definition:

- endpoint – defines the endpoint to which results are returned. This must be a complete and working URL.
- consumerMRN – the MRN of the consumer that submitted the search. Taken from the certificate.
- searchFilterObject – the JSON searchFilterObject in the same format as is used in 4.2.2.

4.4.2. OPERATION POST /API/G1191/V2/UPLOADRESULTS/[TRANSACTIONID]

Used by other MSRs to return results to the originating MSR.

4.4.2.1. Request parameters

No parameters are allowed.

4.4.2.2. Request body

Attribute	Type	Multiplicity	Definition
envelopeSignature	String	1	Envelope signature
envelope	EnvelopeUploadSearchResultObject	1	The actual list of instances found.
EnvelopeUploadSearchResultObject			
serviceInstance	ServiceInstanceObject	0...n	Similar to response to searchService (see **Erreur ! Source du renvoi introuvable.**) with the exception that transactionId is not returned in the body as it is a part of the path

4.4.2.3. Service response

Normal HTTP status code 200 if the data is valid. For any request where the MRN of the sender does not conform to the MSR MRN defined in G1183 (i.e. does not begin with urn:mrn:mcp:msr) a HTTP response with status code 400 must be returned.

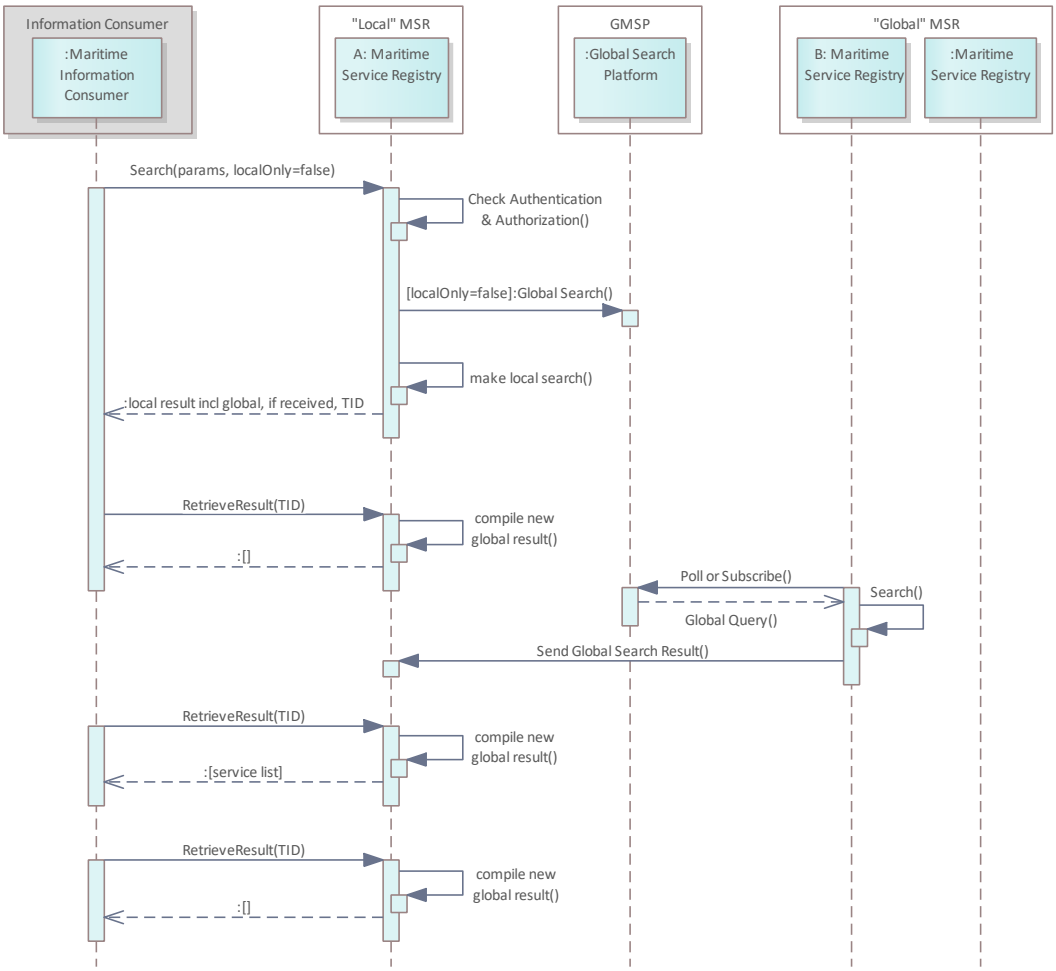

Figure 4 *Service Response*

4.5. INTERFACES REQUIRED IN SERVICES

4.5.1. OPERATION GET /V2/PING

All services registered in MSR must support this interface and supply the URL to it in the instance information to enable service monitoring by the MSR.

4.5.1.1. Request parameters

No parameters are allowed.

4.5.1.2. Service response

HTTP status 200 and message content must be the current timestamp. Other fields may be present in the response.

5. ABBREVIATIONS

JSON JavaScript Object Notation

MCP Maritime Connectivity Platform

MCC Maritime Connectivity Platform Consortium

MIR Maritime Identity Registry

MMS Maritime Messaging Service

MRN Maritime Resource Name

RTCM Radio Technical Commission for Maritime Services

SECOM Secure communication between ship and shore

URI Uniform Resource Indicator

URL Uniform Resource Locator

URN Uniform Resource Name

XML eXtensible Markup Language

6. REFERENCES

[1] IALA Guideline G1128 The Specification of E-Navigation Technical Services

[2] IALA Guideline G1143 Unique identifiers for maritime resources (MRN)

[3] Semantic Versioning https://semver.org/

[4] IALA Guideline G1183 Provision of MCP Identities

[5] IEC 63173-2 Secure communication between ship and shore (SECOM)

[6] RTCM Standard 13900.0 Maritime Messaging Service Architecture and Protocol

ANNEX A MSR OPENAPI SPECIFICATION

The OpenAPI specification of the MSR can be found at IALA website: https://www.iala.int/technical/technical-services/.

ANNEX B MSR SEARCHAREA DEFINITIONS

The geoJSON file documenting the geometries of the search areas defined as subjects can be found at: https://www.iala.int/technical/technical-services/. These search areas are based on the areas of current NAVAREAs, with inland areas added to coverage by editing some of the existing corner points and adding three new areas for uncovered areas.

ANNEX C USE CASES FOR MULTI-DOMAIN MCP SCENARIOS (INFORMATIVE)

The way MCP instances interact with each other, as well as with their associated services, is crucial for the envisaged distributed MCP. This annex intends to support the discussion on the interoperability of multiple MCP instances, each facilitating its own authentication domain.

C 1 INTRODUCTION

To facilitate the discussion on the interoperability of MCP instances, a list of use cases has been compiled in the following sections. To keep things simple, Figure 1 presents an overview of the generic multi-domain MCP environment, including the main actors involved.

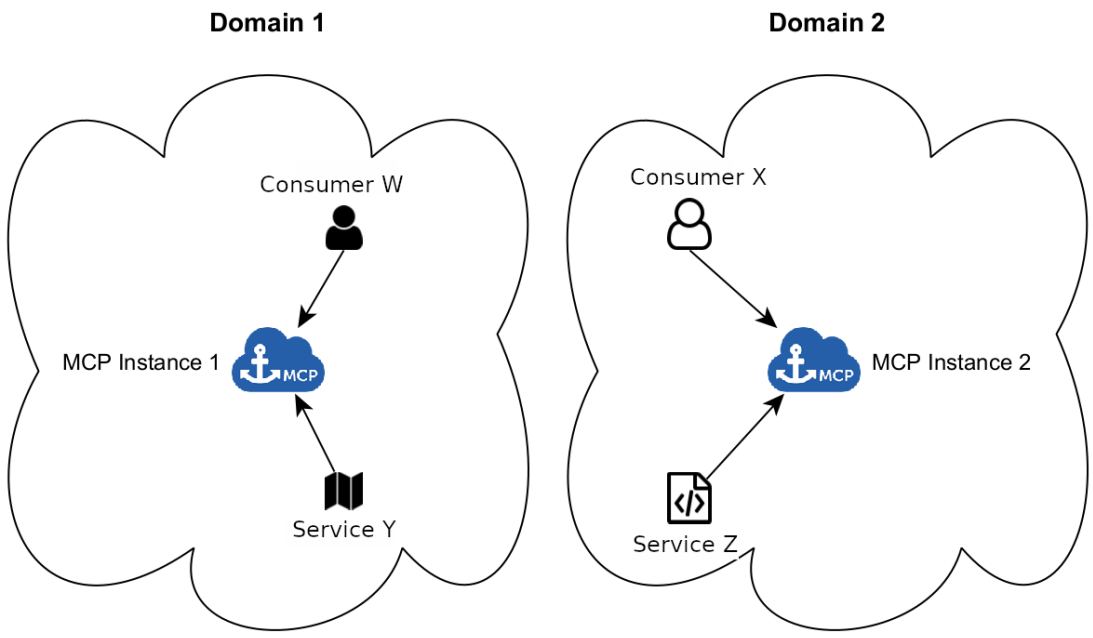

Figure 1 *Overview of a generic environment with multiple MCP domains*

In scenario of Figure 1 we consider two MCP domains. Each domain has one consumer and one service, both associated with the same MCP instance. The overview of the environment does not display the internal components of each MCP instance (i.e. Identity Registry - MIR, Service Registry – MSR, Messaging Service – MMS), for the sake of clarity. We may however refer to them as actors, while describing the operations of each use case. Apart from that however, the involved MCP instances are seen as black boxes, providing the necessary functionality.

In the current context, two MCP domains are considered to be interconnected, when the actors from one domain, can contact and are permitted to interact with the actors of the other. This requires the root Certificate Authority (CA) certificates of each domain to be known and accepted by all actors in the external domain(s).

Table 1 provides a brief description of four different use cases, utilising the environment and actors present in Figure 1. The detailed information on each use case can be found in Section A.22 . This is by no means an exhaustive list, but it represents the most important use cases that have been identified to date.

It should be noted that some use cases may already be included (in part or in full), within the process of other more complex use cases. However, if a use case has merit on its own, it is still be captured and presented independently.

Table 2 Use case overview

Use Case	Description
Use-Case A	A user from an MCP domain wants to discover and use a technical service registered in a different domain.
Use-Case B	A consumer from an MCP domain wants to access data from a technical service registered in a different domain.
Use-Case C	A technical service from an MCP domain wants to validate the identity of a consumer registered in a different domain.
Use-Case D	A consumer from an MCP domain wants to validate the identity of a technical service registered in a different domain.

All digital communications in the aforementioned use cases are assumed to take place over IP, using SSL/TLS encryption (e.g. over HTTPS). This is made possible by employing security certificates of public internet CAs. These are not to be confused with the MCP certificates and MCP CAs. MCP certificates, issued by MCP instances (acting as CAs), are used solely in the context of MCP interactions, in order to verify the validity of requests themselves (including the maritime data transmissions), as per IALA G1183 [1]. An example of this can be found in the IEC SECOM [3] standard.

Finally, an important clarification is that the interactions of a consumer or a service with an MCP instance are not considered to be limited only to actions towards a remote system. For the purposes of this document, any action involving components or functionality of the MCP, including the validation of certificates or signatures and the checks against certificate revocation lists (CRL/OSCP), is considered to be an interaction with an MCP instance.

C 2 USE CASES

C 2.1. USE CASE A – MSR GLOBAL SEARCH

This use case is described earlier in this document.

- Who: A consumer registered with a legitimate MCP instance.
- Wants to: Discover and use a technical service registered in a different MCP domain.
- So that: It will obtain the information required for its task (e.g. plan a route).

C 2.1.1. DESCRIPTION

A consumer W is a registered user of a legitimate MCP instance in Domain 1. They intend to make a trip towards the destination and will need to obtain some information necessary for the trip (e.g. for planning a route, such as Navigational Warnings or AtoN information). To find the appropriate service(s) (service Z) that can provide that information, the consumer performs a search query to their respective MCP, submitting as JSON payload:

- The geometry of interest (e.g. route path);
- The service design MRN (see G1128 [3]) and versions which are compatible with their onboard equipment;
- The service status which should be Released; and
- The local only parameter is set to false.

A visual overview of this use case, making use of the generic environment established previously can be seen in Figure 2Figure 2. The figure includes the numbered steps of the ordinary sequence of events.

C 2.1.2. ACTORS

- User using the consumer information system.
- Consumer (ECDIS, Route-Planning System or other information system).

- Maritime Technical Service (such as for Navigational Warnings, AtoN information) in its own MCP domain.
- MSR service of the consumer's MCP domain.
- MSR service of the technical service's MCP domain.
- Maritime Technical Service (such as for Navigational Warnings, AtoN information) in an external MCP domain.

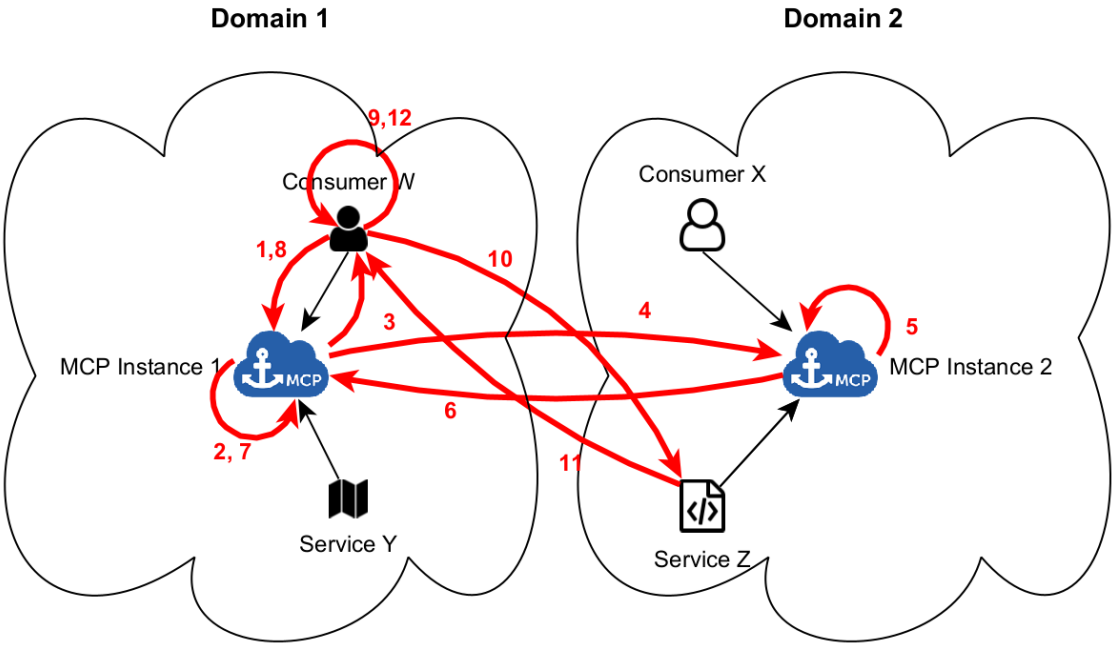

Figure 2 *The outline of the ordinary sequence of events for the Use Case A*

C 2.1.3. FREQUENCY OF USE

Typically triggered when the consumer is performing the task (e.g. planning for a trip) for a destination which is far away from their base of operations.

C 2.1.4. PRE-CONDITIONS

- The consumer is registered with a legitimate MCP instance.
- The consumer's MCP instance is interconnected with a compatible instance associated with a technical service, which meets the consumer's requirements.
- The MCP instance of the technical service is also a legitimate MCP instance.
- All actors support the search service request functionality.
- The consumer of the search has the ability to poll an MSR for further results.
- Identity verification is a given in this use case and is not described.

C 2.1.5. ORDINARY SEQUENCE

1 The consumer sends a search request to the MSR of its own MCP domain, including its route path and other criteria.

2 The consumer's MSR searches its internal database and finds any matching registered entry.

3 The consumer's MSR will reply with the local search result and supply a transaction ID that can be used when returning results from the other MCPs.

4 The consumer's MSR propagates the search request (along with the geometry provided description of the route) to interconnected MCP instances, which potentially have services meeting the requirements specified in the received request.

5 The MSRs of the interconnected MCP instances will validate the request and ensure that it comes from a reliable source, which is already vetted and allowed to request information from the search service.

6 The interconnected MSRs will respond with the search results from their own internal databases. If a search via the search platform does not produce any results, an MSR should not respond with an empty result.

7 The consumer's MSR will collect all valid responses identified by the transaction ID and compile a single list of search response entries.

8 The consumer will receive the service information list by polling the MSR to get the results as they arrive via global search. If no results are received, an empty list is returned.

9 The consumer will select which of the services it will contact, based on its own set of criteria.

10 The consumer will contact the selected technical service (Service Z in the example of Figure 2), sending a request to be processed.

11 The technical service will respond to the consumer with the data matching the request made.

12 The data is rendered and displayed to the user.

C 2.1.6. POST-CONDITIONS

The correct maritime information is received by the consumer.

C 2.2. USE CASE B – TECHNICAL SERVICE INFORMATION RETRIEVAL

- Who: A consumer registered with a legitimate MCP instance.
- Wants to: Access data from a technical service registered in a different MCP domain.
- So that: It will obtain the information required for performing a task (e.g. plan a route).

C 2.2.1. DESCRIPTION

This is a subset of the previous Use Case AUse Case A. It involves the operations that take place when a consumer W needs to access information from a technical service Z, which is associated with a different MCP domain. The initial consumer request to the service should therefore first be validated and if the consumer belongs to a recognised and interconnected MCP domain, then the service should be allowed to respond. Likewise, the consumer is required to ensure that the response, along with any cryptographic signatures, is authentic and still valid.

A visual overview of this use case, making use of the generic environment established previously can be seen in Figure 7. The figure includes the numbered steps of the ordinary sequence of events.

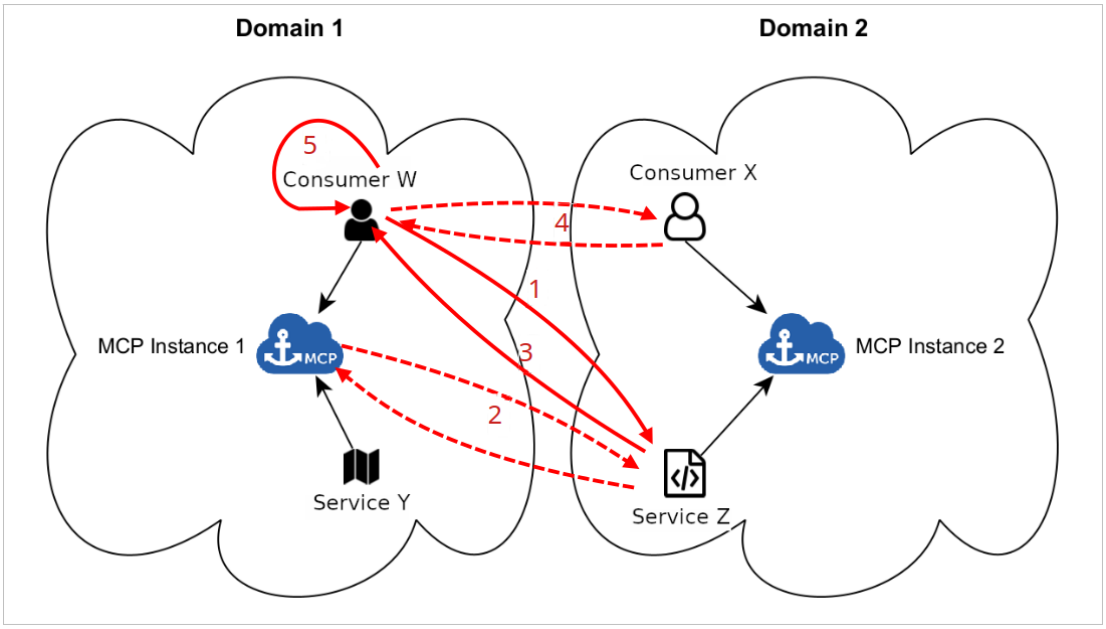

Figure 3 *The outline of the ordinary sequence of events for Use Case B*

C 2.2.2. ACTORS

- User using the consumer information system.
- Consumer (ECDIS, Route-Planning System or other information system).
- Maritime Technical Service (such as for Navigational Warnings, AtoN information) in its own MCP domain.
- The MIR service of the consumer's MCP domain.
- The MIR service of the technical service's MCP domain.

C 2.2.3. FREQUENCY OF USE

Typically triggered when the consumer is required to access information from services that belong to different MCP domains.

C 2.2.4. PRE-CONDITIONS

- The consumer is registered with a legitimate MCP instance.
- The technical service is registered with a legitimate MCP instance.
- The consumer's MCP instance is interconnected with a compatible instance associated with a technical service, which meets the consumer's requirements.
- The consumer has already all the necessary knowledge on how to access the technical service.
- Both MCP instances provide the facilities to validate MCP certificates.

C 2.2.5. ORDINARY SEQUENCE

1 The consumer will send a data retrieval request to the technical service, based on the already known contact information (e.g. from a previous MCP request).

2 The technical service receives the incoming requests and validates the identity of the consumer and the validity of the incoming request. This can be carried out using an OCSP call to the external MIR or via a local copy of the CRL.

3 If the identity of the consumer is indeed valid, the technical service will send back a response with the requested data.

4 The consumer will receive the technical service response and will first have to first validate the identity of the sender. This can be carried out using an OCSP call to the external MIR or via a local copy of the CRL.

5 Once the identity of the sender is verified, the consumer should also check the validity of the incoming data, through the included cryptographic signatures.

C 2.2.6. POST -CONDITIONS

The correct maritime information is received by the consumer and presented to the user.

C 2.3. USE CASE C – CONSUMER IDENTITY VALIDATION BY TECHNICAL SERVICE

- Who: A technical service registered with a legitimate MCP instance.
- Wants to: Validate the identity of a consumer registered in a different MCP domain.
- So that: It can establish a secure communication and allocate the appropriate resources.

C 2.3.1. DESCRIPTION

This particular use case can be considered as a subset of both previous A and B use cases. It involves the operations that take place when a technical service Z needs to verify the identity of a consumer W, which is registered in a different MCP domain. The reason why this interaction was initiated is irrelevant, as it forms part of multiple operations such as data retrievals, subscriptions, notifications etc. Therefore, the identity of the consumer needs to be first validated and if it belongs to a recognised and interconnected MCP domain, then the technical service should be allowed to accept the consumer as a legitimate user.

A visual overview of this use case, making use of the generic environment established previously can be seen in Figure 8. The figure includes the numbered steps of the ordinary sequence of events.

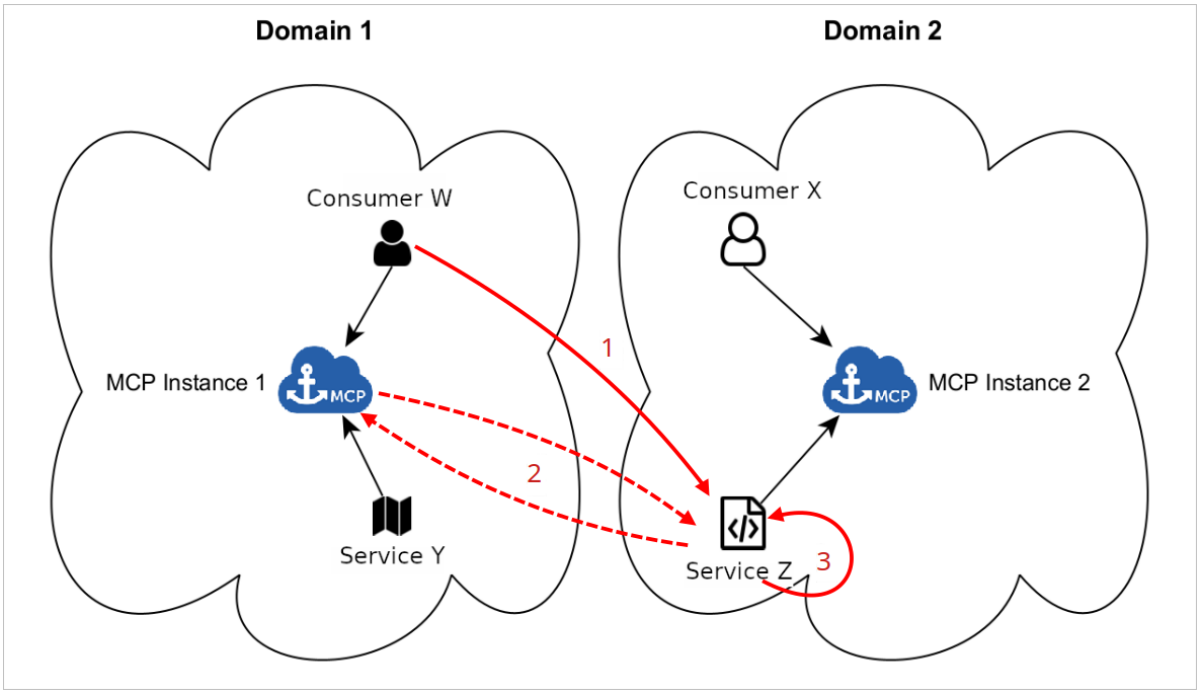

Figure 4 *The outline of the ordinary sequence of events for Use Case C*

C 2.3.2. ACTORS

- User using the consumer information system.
- Consumer (ECDIS, Route-Planning System or other information system).
- Maritime Technical Service (such as for Navigational Warnings, AtoN information) in its own MCP domain.

The MIR service of the consumer's MCP domain.

C 2.3.3. FREQUENCY OF USE

Typically triggered when the consumer is required to send messages to services that belong to different MCP domains.

C 2.3.4. PRE-CONDITIONS

- The consumer is registered with a legitimate MCP instance.
- The technical service is registered with a legitimate MCP instance.
- The consumer's MCP instance is interconnected with a compatible instance associated with a technical service, which meets the consumer’s requirements.
- The consumer already has the necessary knowledge on how to access the technical service.
- The consumer’s MCP instance provides the facilities to evaluate MCP certificates.

C 2.3.5. ORDINARY SEQUENCE

1 The consumer will send a relevant request, regardless of whether it is a get object/subscribe/notification, to the technical service.

2 The technical service will receive the consumer’s request and will first have to validate the identity of the sender. This can be carried out using an OCSP call to the external MIR or via a local copy of the CRL.

3 Once the identity of the consumer is verified, the technical service should also check the validity of the incoming data, through the included cryptographic signatures, before proceeding to process the incoming message.

C 2.3.6. POST-CONDITIONS

The consumer message is received and processed by the technical service.

C 2.4. USE CASE D – TECHNICAL SERVICE IDENTITY BY CONSUMER

- Who: A consumer registered with a legitimate MCP instance.
- Wants to: Validate the identity of a technical service registered in a different MCP domain.
- So that: It can establish a secure communication and trust the transmitted information.

C 2.4.1. DESCRIPTION

This particular use case can also be considered as a subset of both previous A and B use cases. It involves the operations that take place when a consumer W needs to verify the identity of technical service Z, which is registered in a different MCP domain. The reason why this interaction was initiated is irrelevant, as it forms part of multiple operations such as data uploads, subscriptions, notifications etc. Therefore, the identity of the technical service needs to be first validated and if it belongs to a recognisable and acknowledged MCP domain, then the consumer should be allowed to accept the technical service as legitimate.

A visual overview of this use case, making use of the generic environment established previously can be seen in Figure 9. The figure includes the numbered steps of the ordinary sequence of events.

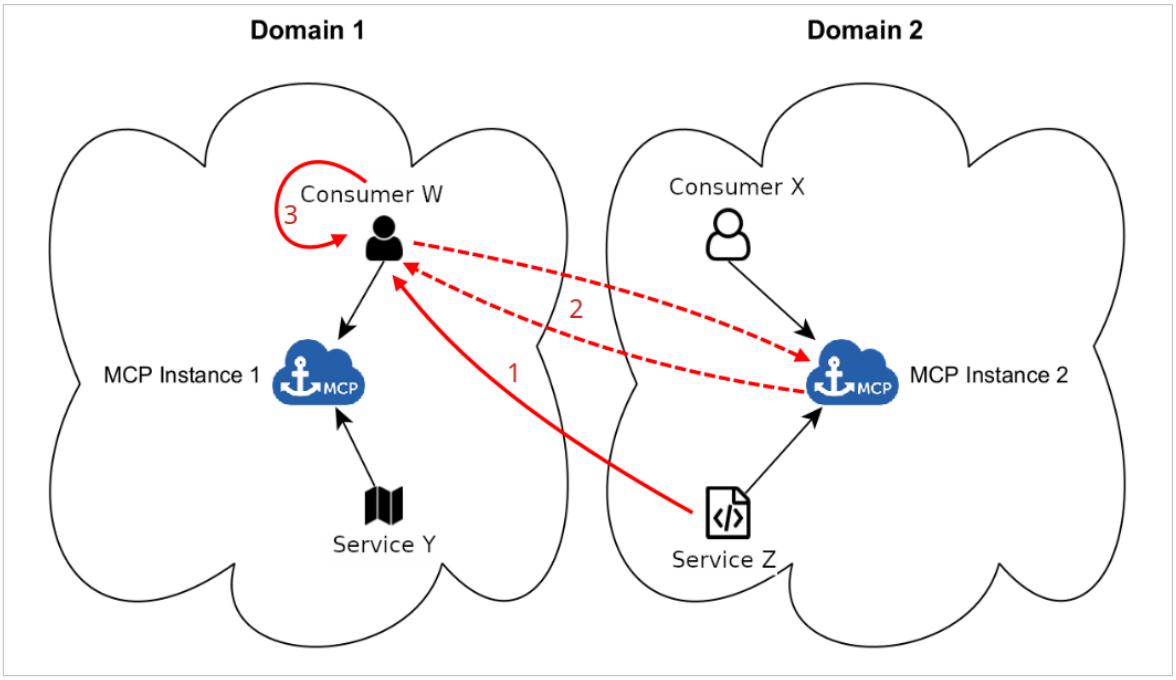

Figure 5 *The outline of the ordinary sequence of events for Use Case D*

C 2.4.2. ACTORS

- User using the consumer information system.
- Consumer (ECDIS, Route-Planning System or other information system).

- Maritime Technical Service (such as for Navigational Warnings, AtoN information) in its own MCP domain.
- The MIR service of the technical service's MCP domain.

C 2.4.3. Frequency of Use

Typically triggered when technical services need to communicate with consumers that belong to different MCP domains.

C 2.4.4. Pre-Conditions

- The consumer is registered with a legitimate MCP instance.
- The technical service is registered with a legitimate MCP instance.
- The consumer's MCP instance is interconnected with a compatible instance associated with a technical service, which meets the consumer's requirements.
- The technical service already has all the necessary knowledge on how to access the consumer.
- The technical service's MCP instance provides the facilities to evaluate MCP certificates.

C 2.4.5. Ordinary Sequence

1 The technical service will send a relevant request, regardless of whether it is an upload/response/notification, to the consumer.

2 The consumer will receive the technical service message and will first have to validate the identity of the technical service. This can be carried out using an OCSP call to the external MIR or via a local copy of the CRL.

3 Once the identity of the technical service is verified, the consumer should also check the validity of the incoming data, through the included cryptographic signatures, before proceeding to process the incoming message.

C 2.4.6. Post-Conditions

The technical service message is received and processed by the consumer.