ETSI GS CDM 004 V1.0.0 (2021-09)

Common Information sharing environment service and Data Model (CDM); Service Model

Disclaimer

Reference

DGS/CDM-004

Keywords

data sharing, maritime, safety, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) european Common information sharing environment service and Data Model (CDM).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

In order to be able to effectively perform the information exchanges required, CISE Participants need to agree on a set of semantics to communicate and share the relevant elements from the Data Model. The way in which such communication is specified is described in the present document as the CISE Service Model.

1   Scope

The present document defines the Service Model protocols for the Common Information Sharing Environment Service and Data Model (CDM Protocols).

2   References

2.1   Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

The following referenced documents are necessary for the application of the present document.

[1]   ETSI GS CDM 005: "Common Information sharing environment service and Data Model (CDM); CDM Data Model".

[2]   ISO 3166 1: "Country codes".

[3]   W3C® Recommendation 11 April 2013: "W3C recommendation XML Signature Syntax and Processing".

NOTE: Available at https://www.w3.org/TR/xmldsig-core/.

[4]   W3C® Recommendation 12 February 2002: "XML-Signature Syntax and Processing".

NOTE: Available at XML-Signature Syntax and Processing (w3.org).

[5]   W3C® Recommendation 15 March 2001: "Canonical XMLVersion 1.0".

NOTE: Available at Canonical XML (w3.org).

[6]   Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

2.2   Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[i.1]   ETSI GS CDM 003: "Common Information sharing environment Service and Data Model (CDM); CDM Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

access right matrix: tool used to link each service and entity provided by Participants on the Node with all the possible consumers

> NOTE: It ensures that a service is not available to all the Participants belonging to a given Community or that one of the entity's attributes exchanged by the service is not allowed to a given Participants and need to be removed by the response provided by the service.

activity: activity performed by a sector

adaptor: component external to CISE network connecting a Participant to CISE network via standardized interface

> NOTE 1: The Adaptor is the bridge between the Legacy System and the Gateway translating LS data to the CISE Data Model. The Adaptor uses available Gateway Services depending on the strategy chosen for message exchange patterns and Data Model.

> NOTE 2: The Adaptor could be either software or software/hardware component.

> NOTE 3: In case of a new system connected to CISE, the Adaptor functionality may be part of the new system.

artemis: queueing component

> NOTE: Developed by the Apache Software Foundation (https://activemq.apache.org/components/artemis/).

certification authority: entity issuing digital certificates, authenticating the ownership of a public key by the named subject of the certificate

classified: sensitive information to which access is restricted by law or regulation

consul: tool for discovering and configuring services in existent SOA infrastructure

consumer: participant requesting Services over CISE network, only consuming but not providing information

coopP: project financed by the European Commission in 2013 defining the CISE use cases and the first version of the CISE data and service model

> NOTE: See https://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance_en for more information.

cross-sector: exchange of information between two or more sectors

cross-border: exchange of information between EU or EFTA countries

EUCISE2020: FP7 pre-operation validation project on CISE

> NOTE: The project defined and developed the existing CISE Network and software (2014-2019).

EU RESTRICTED: classified information covered by the definition of EU security classification levels

> NOTE 1: EU classified information is any information or material designated by the EU security classification, the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

> NOTE 2: The following EU security classification levels are defined:

> > ▪ EU TOP SECRET: information and material the unauthorized disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

■   EU SECRET: information and material the unauthorized disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

■   EU CONFIDENTIAL: information and material the unauthorized disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

■   EU RESTRICTED: information and material the unauthorized disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

information system: system designed to collect, process, store, and distribute information

key-value storage: data storage paradigm designed for storing, retrieving, and managing associative arrays, and a data structure more commonly known today as a dictionary or hash table

legacy system: software designed to perform specific tasks and that exposes certain functionalities through interfaces in the domain of the maritime surveillance

> NOTE: In the present document, Public Authorities maintain Legacy Systems. Legacy Systems are the originator and final destinations of messages exchange in CISE.

message: one of the structured sentences exchanged between Participants to discover, request and provide Services

national information system: information system related to the specific Member State

node: software components that provide CISE infrastructure and access point to CISE network

node administrator: role assumed by a User to manage the CISE Node software, hardware and network connections

node agent: Operating Entity that operates on the Node

node configuration manager: role assumed by a User to manage the declaration of services in the CISE network

node service manager: infrastructure service responsible to manage web services on CISE

participant: legacy System connected to the CISE network for exchanging data supporting one or more of the seven Sectors in performing their Activities

provider: participant providing Services over CISE network

public authority: any organization or legal entity that has an interest in maritime surveillance information

> NOTE 1: An authority can be local, regional, national or European.

> NOTE 2: This organization may have responsibilities linked to one of the seven sectors of maritime surveillance.

public key certificates: digital certificate or identity certificate used in cryptography as an electronic document to prove the ownership of a public key

> NOTE 1: The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified that the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

> NOTE 2: A Public Key Infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates. The PKI creates digital certificates that map public keys to entities.

> NOTE 3: In a typical Public-Key Infrastructure (PKI) scheme, the signer is a Certification Authority (CA).

regional information system: information system related to a specific Area (region)

sector: user community involved in maritime surveillance

> NOTE: The seven sectors are the following:

■   Maritime Safety, Security and Prevention of Pollution by Ships

■   Fisheries Control

- ▪ Marine Pollution Preparedness and Response, Marine Environment

- ▪ Customs

- ▪ Border Control

- ▪ General Law Enforcement

- ▪ Defence

sea basin: sea area

NOTE: The following sea areas are identified:

- ▪ Atlantic

- ▪ Baltic Sea

- ▪ North Sea

- ▪ Mediterranean

- ▪ Black Sea

- ▪ Outermost Regions

- ▪ Arctic Ocean

service: formalized way to exchange information between Participants in CISE network following Service Oriented Architecture (SOA) principles

service registry: registry where services provided by the CISE Adaptors connected to a Node are registered and managed

NOTE: Each CISE Node has its own Service Registry.

site: physical place where CISE Node is deployed

state-of-the art security configuration: most recent stage in security measures implemented to reduce cyber vulnerabilities

unclassified: information to which access is not restricted by law or regulation

user: person appointed by the Public Authorities, interacting directly with CISE or with a Legacy System connected to CISE

3.2   Symbols

Void.

3.3   Abbreviations

For the purposes of the present document, the following abbreviations apply:

AIS	Automatic Identification System
C2	Command and Control system
CC	Carbon Copy
CISE	Common Information Sharing Environment
CSDP	Common Security and Defence Policy
EU	European Union
LS	Legacy System
MRCC	Maritime Rescue and Coordination Centre
PKI	Public Key Infrastructure
REST	Representational State Transfer

SAR   Search And Rescue
SOA   Service Oriented Architecture
SOAP   Simple Object Access Protocol
SQL   Structured Query Language
TCP   Transmission Control Protocol
TEU   Treaty on European Union
TLP   Traffic Light Protocol
URL   Uniform Resource Locator
UTF   Unicode Transformation Format
UUID   Universally Unique Identifier
VTM   Vessel Traffic Management
XML   eXtensible Markup Language
XSD   XML Schema Document

4   Overview

The present document presents the Service Model protocol and underlying semantics for the information sharing environment Architecture identified in ETSI GS CDM 003 [i.1].

The decentralized information exchange system is directed to interlink all relevant Sectors, taking into account existing sectoral information exchange networks and planned system, and allowing for the improvement and development of both the existing sectoral systems, and the overarching CISE network architecture.

The network vision concept is that each Member State and Sectors can adopt one of the following paradigms:

- **One-way approach:** all public authorities in a Member State are connected to the CISE network through a single access point.

- **Multi-way approach:** the public authorities of a Member State are connected to the CISE network through different access points.

The CISE environment is designed to allow the interoperability of national or European legacy systems belonging to public authorities in the Member States through two components:

- **CISE Adaptor**, which allows an information legacy system to connect to a CISE Node. It converts data into the common CISE data model.

- **CISE Node**, which implements common CISE specifications and implements CISE messaging protocol for exchange with the CISE adapter or other CISE Nodes.

The services developed in CISE are organized into two classes:

- **Infrastructure (Core Services)**, which represent the basic services implemented by the CISE Node in order to ensure the connection of each partner, or group of them, to the CISE network.

- **Interface (Common Services)**, which are dedicated to the transfer of entities within the CISE network following the CISE rules.

In accordance with the aforementioned, CISE implements the network architecture defined in [i.1] and also shown in Figure 1:

- The CISE national component is able to connect to the CISE network one or more public authority of the same Member State. In this configuration, the CISE national component acts as a Node and hosts the Infrastructure and Interface services.
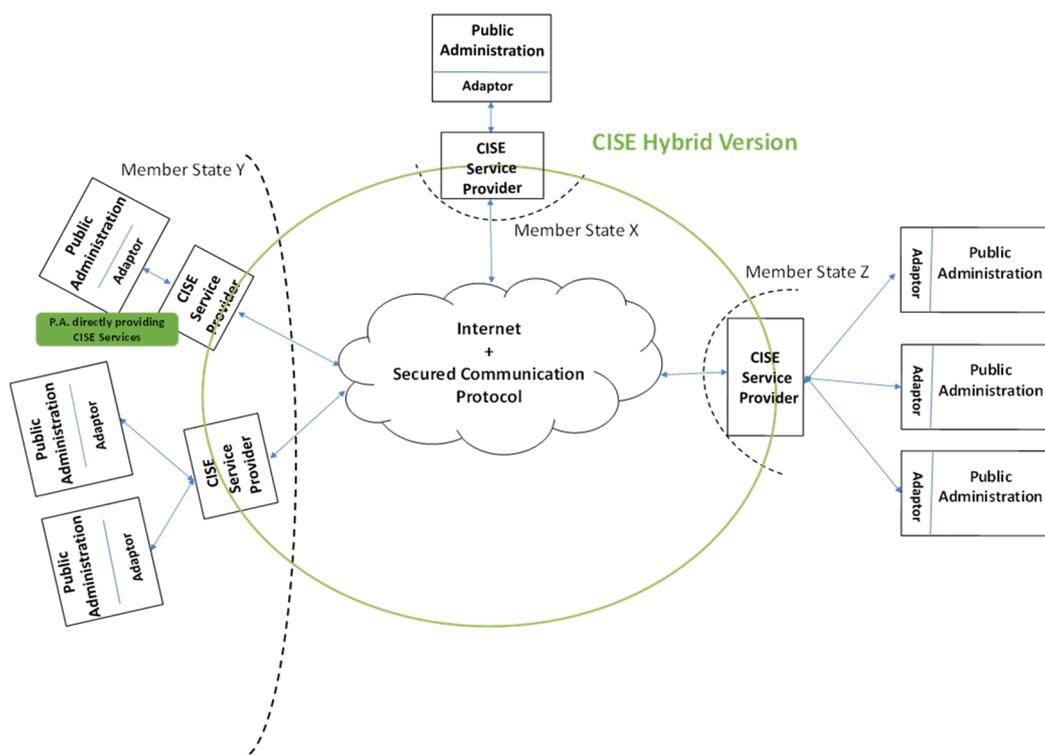
Figure 1: CISE Vision - High Level Operational Concept

The exchange of information between participants is carried out on the basis of a model which provides the following functions:

- **Pull:** the consumer knows the exact list of suppliers and asks for information; the information requested is made available only if and when possible after verifying that the requesting agency is authorized to process the data.

- **Pull Unknown Recipients:** the consumer does not know the exact list of providers and asks for information of interest to all possible suppliers participating in the CISE network. The information is made available only if and when possible after verifying that the requesting agency is authorized to process the data. In this case, different responses to the request may occur.

- **Push:** the provider knows the exact list of consumers and sends them the information regardless of whether they have previously requested this information.

- **Push Unknown Recipients:** the provider does not know the list of consumers, and then sends the information to the node that takes care of sending it to a list of consumers chosen according to the rules defined by the community to which they belong, for the purpose, the type of entity and the subscription of the available services.

- **Publish:** the provider shares a list of information provided to the system periodically to a list of consumers who have subscribed to the service.

- **Subscription:** the consumer subscribes to a service to automatically receive information about an entity, area or community.

The Interface Services, while using the defined message exchange patterns, allow the following business activities:

- **Pull Request:** Query data about an entity/service.

- **Pull Response:** Return data previously requested in a Query.

- **Pull Request subscribe and unsubscribe:** Subscribe and unsubscribe information about an entity/service.

- **Pull Request get subscribers:** Request all the participants subscribed to a service.

- **Push:** Notify about information either resulting from a previous subscription or to unknown destinations.

- **Feedback:** Provide feedback on information already received or sent.

- **Acknowledgement:** Provide success or error messages upon delivery of a message during the transfer process.

- **Discovery:** Discover other services in the CISE network that match the requested profile.

Therefore, the CISE Service Model, the object of the present document, defines how data is exchanged between different partners, in terms of communication protocol and data structures.

5   The CISE Service Model

5.1   Overview

The Service Model is divided into three packages of data structures: Authority, Message and Service. A CISE Service Model implementation shall thus provide:

- An implementation of the CISE communication patterns:
  - Message flow needed to use CISE services.
  - Message Parameters.
  - Expected return values.

- An implementation of relevant Interfaces:
  - Node-Node.
  - Adaptor-Node.

- An implementation of the relevant Information Security constraints:
  - Integrity, non-repudiation: signatures.
  - Confidentiality: encryption.

- Support for the CISE Service Model Data Structures:
  - Message description: Message type, sender, recipient, payload, etc.
  - Service description: Service identification, description, type, features, etc.
  - Participant description:
    - System/Adaptor information: endpoint, description, etc.
    - Authority information: contact information, etc.
    - CISE Node information.

5.2   CISE Services

Each CISE service shall offer a set of operations to support the exchange of the data entities as defined in the CISE communication patterns. Service providers will choose which operations should be implemented according to their needs. Additionally, a Feedback operation allows authorities to communicate issues in the information exchanged previously, and shall be supported as well.

The Operations, their Parameters and expected Return values for each operation are described in Table 1.

Table 1: Operations, Parameters and Return Value

Operation	Description	Parameters	Return Value
Pull	This operation is used to request information using a query-by-example mechanism.	Data template (including the main entity of the service) Capabilities requested	Acknowledgement A list of [Main Entity] + [Entities directly related to the main one] Capabilities offered
Push	This operation is used to push information to a CISE consumer. The origin of the notification might be a previous subscription.	A list of [Main Entity] + [Entities directly related to the main one] Capabilities offered	Acknowledgement
Subscribe	This operation is used to subscribe or unsubscribe to a series of notifications on specific information.	Data template (including the main entity of the service) Capabilities requested	Acknowledgement Capabilities offered
Feedback	This operation is used to provide feedback on information already exchanged.	Reference to previous exchange Nature of the issue	Acknowledgement

Service Providers should register their services (along with the characteristics described above, including a template of the available information) in the CISE Service registry. The registration will help other CISE participants to understand what can be expected from the service.

5.3   CISE Services and Messages Definition

A CISE Node shall implement the relevant CISE entities for its planned service and usage requirements.

In the following diagrams the most relevant CISE entities are listed: the Service and the Message.

The Service shall be described in terms of the Participant providing the service and the Service Capability. To route the information, the Message entity has a Sender, a Recipient and CC Recipients which are Services.

CISE has several specializations of the Message, but only the PullRequest extension and the Push contains a ServiceProfile relationship, which allows the "unknown" pattern: the recipient of the message can be determined based on a profile. The payload of the message is represented by the CoreEntityPayload entity.

A simplified class model
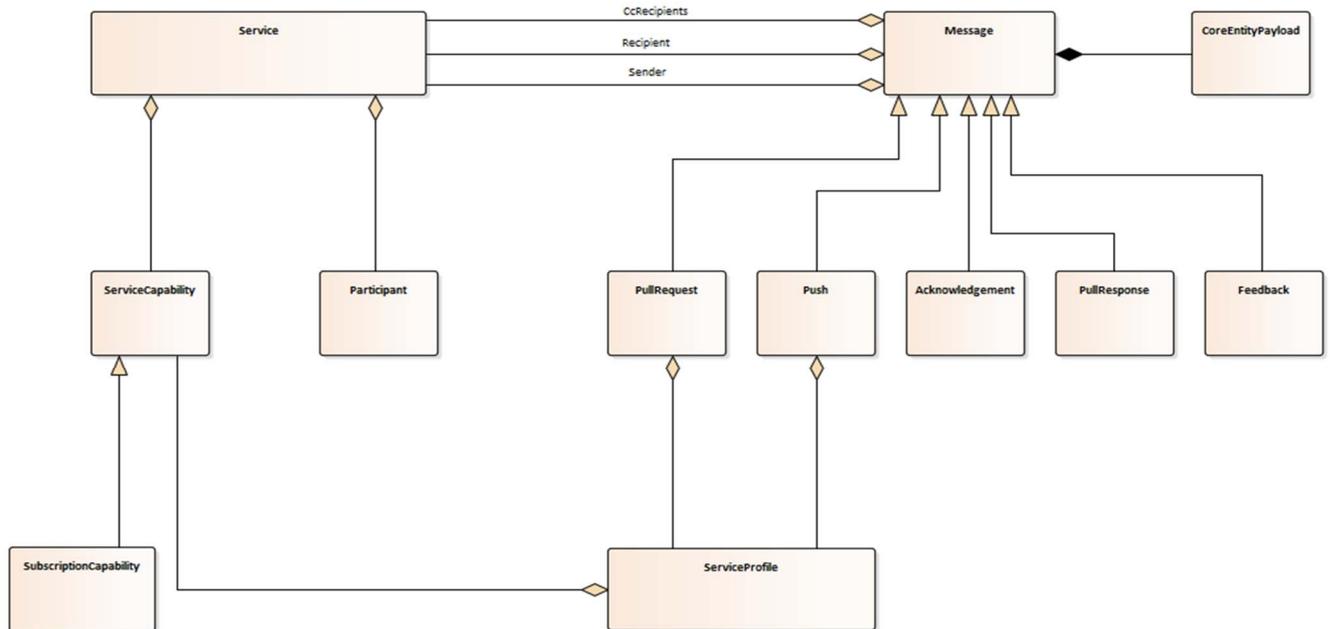
Figure 2: CISE simplified Class Model

Each Service shall be characterized by a ServiceType that implicitly maps it to an underlying Data Model entity as specified in ETSI GS CDM 005 [1], and a series of state definition relationships that will be used both for search and retrieval of the Service for a given interest community in CISE.

These relationships shall be such as ServiceStatus, ServiceRole, DataFreshness, as well as a ServiceCapability description and, when used into an exchange, the ServiceOperation being invoked. These are described in Figure 3.
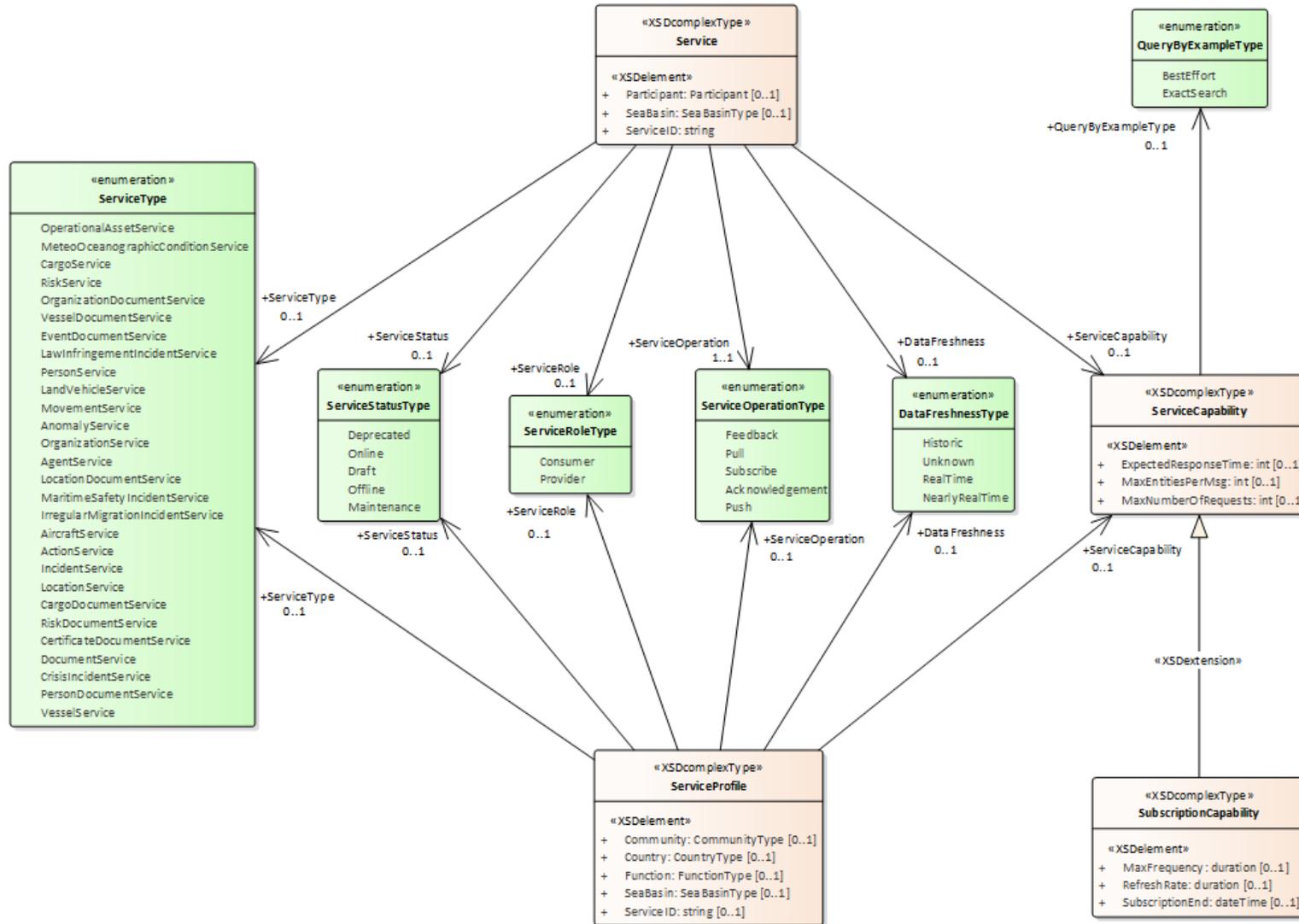
The CISE service model (extract)

Figure 3: Service metadata

A ServiceProfile structure shall allow the characterization of a given type of Service to a given usage pattern, namely its configuration within a given CISE community and be used as a basis for access rules and node configuration, including metadata describing the profile of the service provider, characteristics of the data provided (e.g. freshness) and the data entities supported by the service (including the main entity).

Additionally Service providers should be able to define which information will be available through the service, i.e. which attributes and relationships of the main entity will be provided via an Entity Template, and the Service Capabilities (e.g. max. connection number, max. delay time, etc.).

A Participant shall be characterized by its own definition data, plus a series of relationships with relevant CISE Service Model entities corresponding to the Services the Participant contributes and/or accesses in the CISE network.

A Participant additionally shall specify the PointOfContact responsible for its participation, as well as the Node/Gateway used, as well as providing the classification of the relevant community attributes in its relationships.
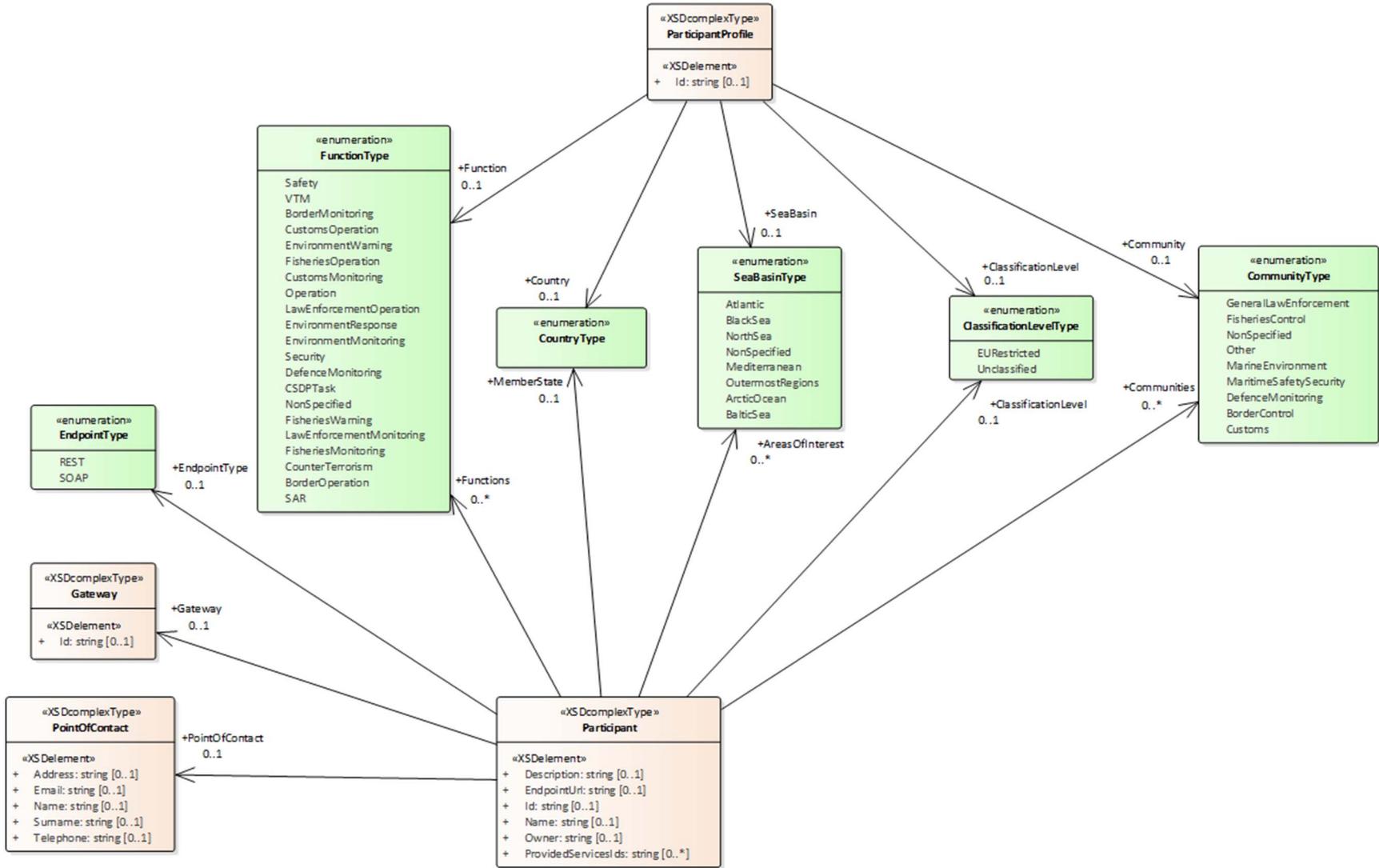
Figure 4: Participant metadata

The CISE Service Model message structure is defined as in Figure 5.
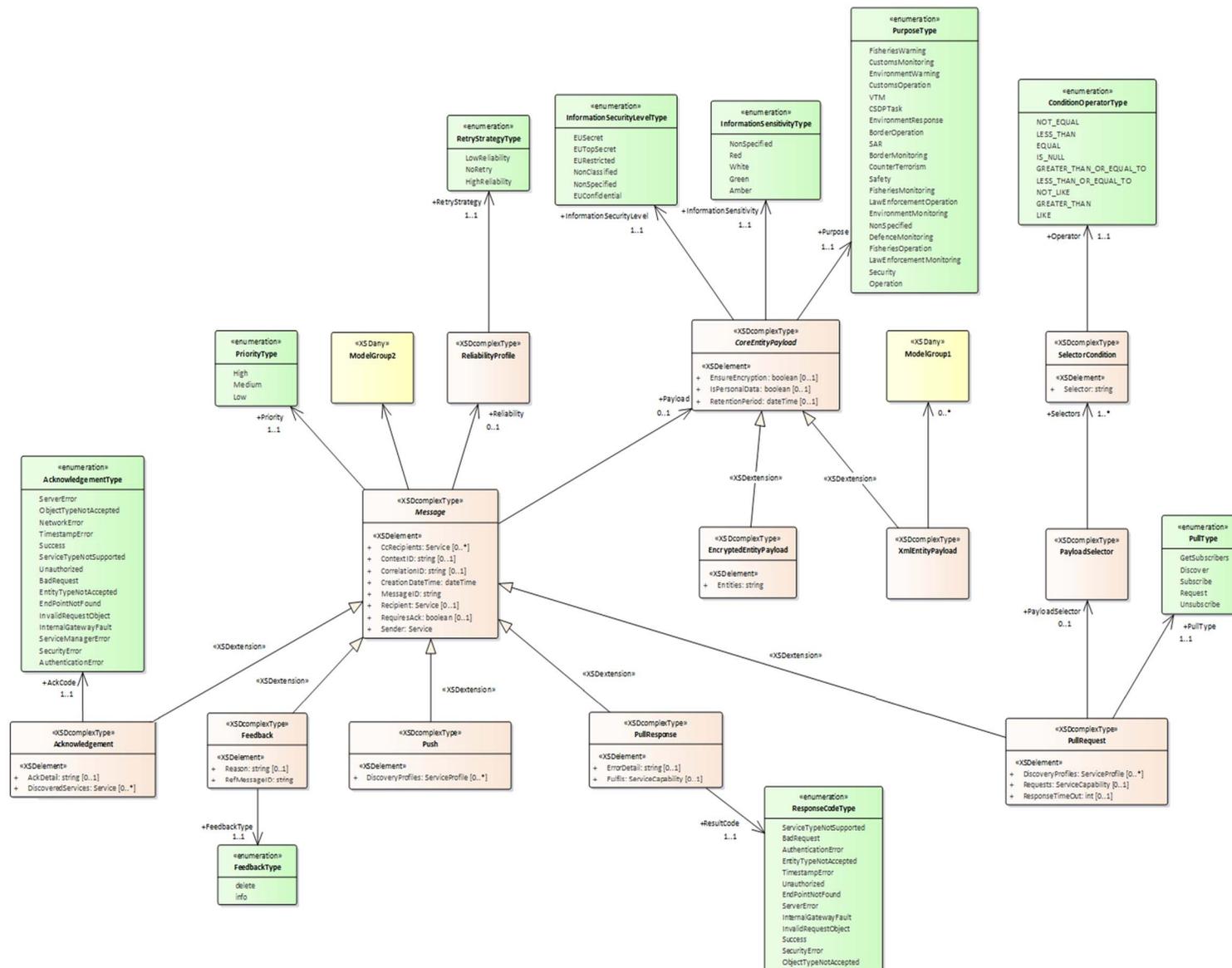
Figure 5: Message structure

5.4   CISE Communication Patterns

5.4.1   Overview

A Node shall implement the relevant CISE Communication Patterns. In CISE, five communication patterns describe how the CISE stakeholders can interact to exchange information between their supporting system. The choice among them will depend on the operational context. Each of these messages shall include a valid CISE Entity payload as specified in the CISE Data Model [1]. In the following clauses an overview for each of them is given.

5.4.2   Pull

The Pull pattern (Figure 6) is based on the *need-to-know* principle. In this pattern, the CISE consumer requests a piece of information to the CISE provider through the Pull operation using the PullRequest message. The CISE provider shall reply using the PullResponse of the CISE consumer.
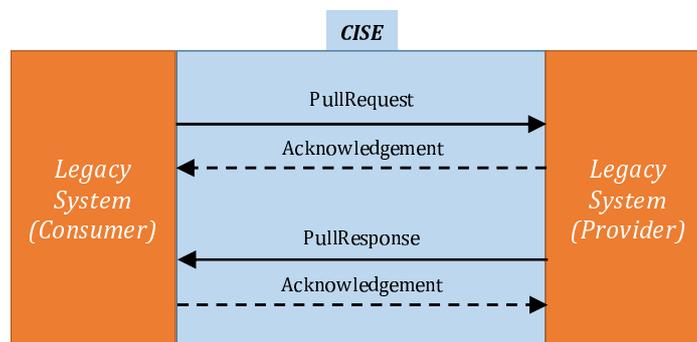
Figure 6: Pull Request/Pull Response

5.4.3   Multicast Pull

In the multicast pull pattern, the CISE consumer shall request a piece of information to a group of CISE providers using the PullRequest operation. The CISE providers might be known previously or the CISE consumer could look for providers using the CISE Authority/Service Registry.
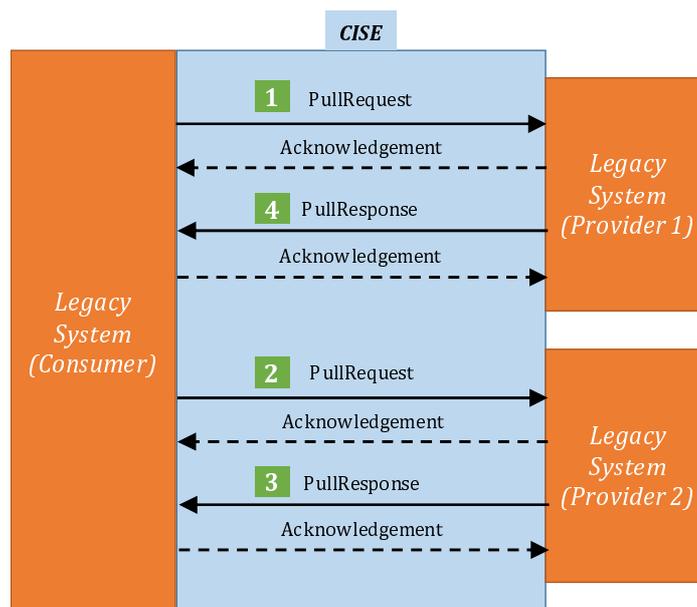
Figure 7: Multicast Pull

5.4.4   Push

The Push pattern (Figure 8) is based on the responsibility-to-share principle. In this pattern, the CISE provider shall send a piece of information to the CISE consumer (which might be of interest) using the Push operation and message.
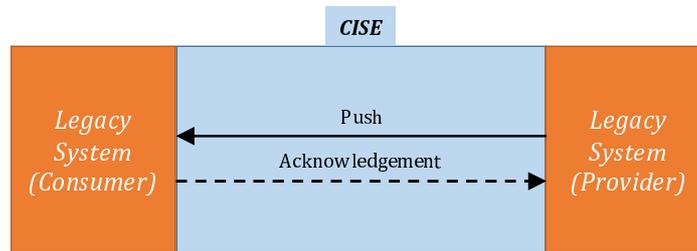
Figure 8: Push

5.4.5   Multicast Push

In the Multicast Push pattern (Figure 9), the CISE provider shall send a piece of information to a group of CISE consumers (who might be interested in it) using the Push operation.
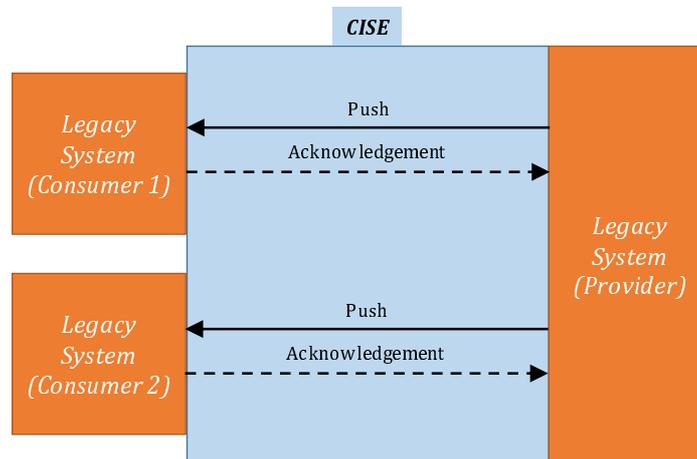
Figure 9: Multicast Push

The CISE consumers might be known previously or the CISE provider could look for consumers using the CISE Authority Registry.

5.4.6   Publish/Subscribe

The Publish/Subscribe pattern (Figure 10) results from the combination of the *need-to-know* and *responsibility-to-share* principles. In this communication pattern, the CISE consumer subscribes to a piece of information from the CISE provider using the PullRequest operation with the *subscribe PullType*. When the piece of information is available in the CISE provider, the provider notifies all the subscribers.
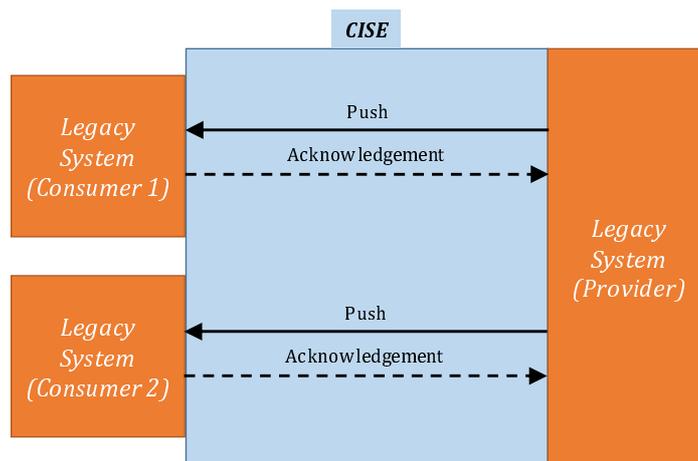
Figure 10: Publish/Subscribe

5.5   CISE Discovery mechanism

In the different communication patterns described above, the consumer knows who the providers are (in the Pull pattern) or that the provider knows who the potential consumers are (in the Push pattern). In reality, the organization and the missions of each authority vary a lot from one Member State to the other. Hence it is difficult to know who can offer what service in advance.

CISE offers a discovery mechanism. This mechanism allows to define two additional communication patterns:

The **PULL UNKNOWN:** allowing for a consumer to request information to one or several providers without knowing in advance which one can answer the request.

The **PUSH UNKNOWN:** allowing a provider to push information to one or several potential interested consumers without knowing in advance who may be interested in receiving this information.

After going through the discovery mechanism, the PULL UNKNOWN may lead to a PULL pattern or a MULTICAST PULL pattern. The same way, the PUSH UNKNOWN may lead to a PUSH or MULTICAST PUSH pattern.

5.6   Service Behaviour

5.6.1   Overview

Clauses 5.6.2 to 5.6.6 describe what entities are expected to be exchanged depending on the way the service has been declared in the Service Registry. These rules shall be implemented in the adaptor of the Legacy System Node providing the information.

The behaviour is illustrated by a set of examples based on the declaration in the service registry as shown in Figure 11 below.
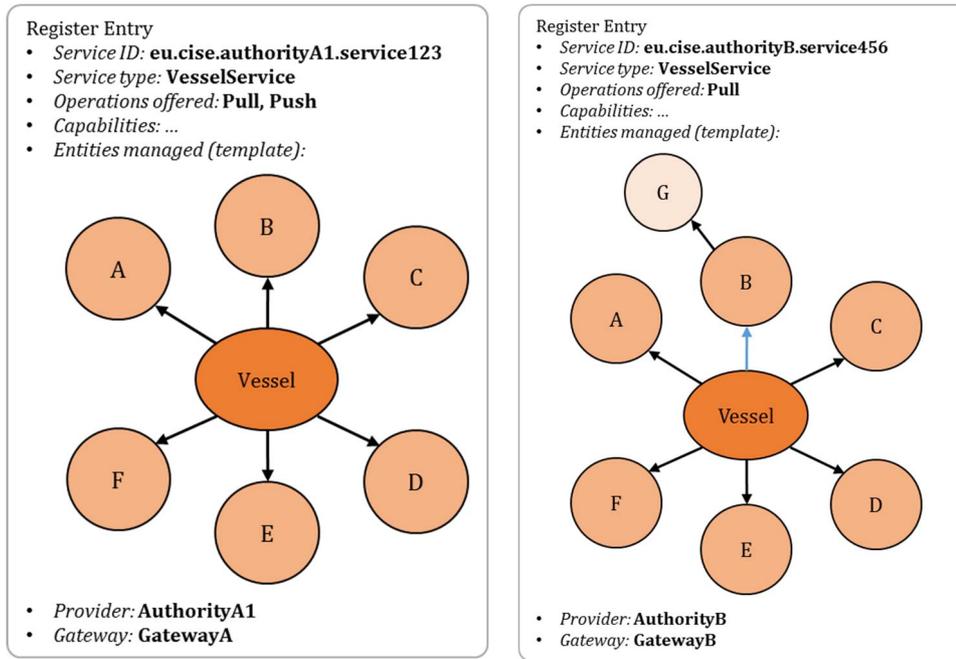
Figure 11: Service behaviour example

5.6.2 Pull

The specification of the Pull operation for the Pull and Multicast Pull patterns use a query-by-example mechanism. Using this mechanism, CISE consumers shall request to a CISE provider all the data entities that are similar to a given example.

Figure 12 shows an example in which the CISE consumer sends to a CISE provider a Vessel entity whose name is "Queen Mary" as the input of the PullRequest operation. The CISE provider should reply with all the Vessel entities whose name is the given one.
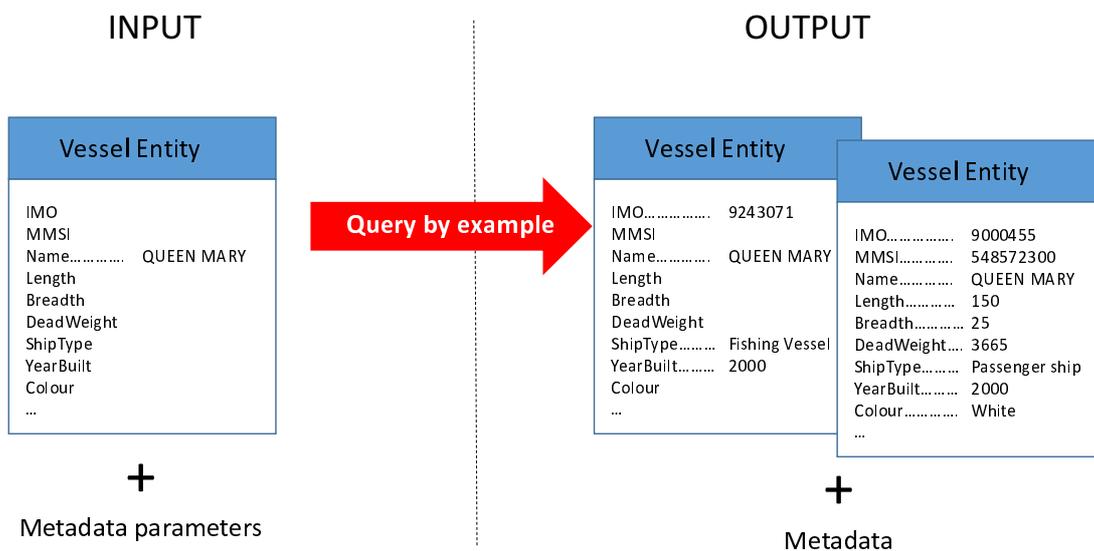
Figure 12: Query by example

In order to limit the complexity of the service operation and streamline its implementation in CISE, the following recommendations are proposed:

- **Only one level of entity relationships.** The entity payload of any **Request** message should only contain one type of data entity and the data entities directly related to it. For instance, according to the CISE Data Model, a service can transmit the Vessel involved in an Incident (Incident-Vessel relationship) but it would not be possible to transmit the Vessel with its cargo involved in an incident (Incident-Vessel-Cargo relationships) with a single service. The Cargo related to the Vessel should be exchanged in a second step. Nevertheless, several entity relationships can be transmitted at the same time, for instance: the Vessels involved in an Incident along with the MRCC in charge of the incident and the location of the incident.

- **Best match.** The CISE providers should deliver a PullResponse message containing data entities that are the most similar to the requested query-by-example entity contained in the corresponding PullRequest message. ServiceCapability parameters are required to indicate which kind of response (QueryByExampleType) is required/delivered, i.e. exact or best match. This property is declared in the Service Registry.

- **Full vs. partial response.** Open queries can result in a high number of responses, or in large responses, which could slow down (or even block) the provider's systems or the CISE network. In order to avoid this problem, some metadata within the service capabilities is also required to indicate the maximum number of responses (MaxEntitiesPerMsg). The provider may also want to restrict the number of responses transmitted for each exchange. This property is declared in the Service Registry (see clause 6.4).

In Table 2, specific case examples are provided for the Pull Request message.

Table 2: Types of Pull Request use cases

Case		Input	Output
Basic pull request	C1	A list of entities that match the input template (exact match).	A list of entities that match the input template (exact match).
	C2		A list of entities that match the supported template according to the service definition.
Pull request with attribute filter	C3	An entity template supported by the service provider (with a subset of the relationships) with a filter in one of the attributes.	A list of entities that match the input template (exact match).
	C4		A list of entities that match the supported template according to the service definition.
Not supported templates (error cases)	C5	Wrong main entity	Error
	C6	Template with a relationship not supported in the service definition	Error
	C7	Template with a 2nd level relationship	Against the recommendation, but results are provided.

In Table 3, specific case examples are provided for the Pull message.

Table 3: Pull Request Examples

Service	Case	Example	
		Input	Output
eu.cise.authorityA1. service123 pull	C1		

Service	Case	Example	
		Input	Output
eu.cise.authorityA1. service123 pull	C2		
eu.cise.authorityB. service456 pull	C1		
eu.cise.authorityA1. service123 pull	C3 C4		
eu.cise.authorityA1. service123 pull	C5		Error: Main entity not found.

Service	Case	Example	
		Input	**Output**
eu.cise.authorityA1. service123 pull	C6		Error: Z not supported.
eu.cise.authorityA1. service123 pull	C7		Error: Only direct relationships are supported.

5.6.3   Push

In Tables 4 and 5, specific case examples are provided for the Push messages:

Table 4: Types of Push use cases

Case		Input	Output
Normal notification	C1	List of entities according to the template supported in the service definition.	Acknowledgement
Entities not according to the service template	C2	List of entities. Some entities contain relationships not supported in the service definition.	Acknowledgement
	C3	List of entities. Some entities contain second level relationships.	Acknowledgement
Not supported templates (error cases)	C4	List of main entities not supported by the service definition.	Error

Table 5: Push examples

Service	Case	Example	
		Input	**Output**
eu.cise.authorityA1. service123 push	C1		Acknowledgement
eu.cise.authorityA1. service123 push	C2		Acknowledgement Z could be discarded by the consumer.
eu.cise.authorityA1. service123 push	C3		Acknowledgement. Z could be discarded by the service provider
eu.cise.authorityA1. service123 push	C4		Error: Main entity not found.

5.6.4   Subscribe

The Publish/Subscribe pattern consists of three independent communication processes:

- **Subscribe:** the CISE consumer subscribes to a piece of information of the CISE provider using the Pull operation. In this case, the PullRequest message should indicate that it is a subscription process (PullType = subscribe). The CISE provider will register the CISE consumer and will send back a correlation ID (correlationID) in the PullResponse message.

- **Publish:** When the CISE provider wants to make available a piece of information (e.g. a list of data objects), the provider Node needs to check the list of subscribers (CISE consumers). Subsequently, to each subscriber, the provider sends a Push message with the correlation ID provided before.

- **Unsubscribe:** The subscription can last for a time period given in the ServiceCapability parameter (SubscriptionDuration) or until the CISE consumer unsubscribes using the PullRequest message (PullType = unsubscribe).

5.6.5   The Multicast Patterns

The multicast patterns enable the CISE participants to request or send information to more than one participant. There are two main aspects in the management of the multicast communications:

- **Identification of the target participants:** In order to start the information exchange, the CISE participants should identify the target participants at the other end. For this, the DiscoveryProfile has to describe the criteria for selecting the target participants according to the services they offer. The CISE Node will search the identity of the target participants in the Authority and Service registries.

- **Independent communication between participants:** The exchange between two participants (e.g. A - B) is independent from the other exchanges (e.g. A - C, A - D, etc.). For instance, the retry mechanism, the acknowledgement protocol or the errors (among others) should be managed independently.

5.6.6   The Service Discovery Mechanism

The Legacy System may notify or request information to a sub-group of CISE participants. This can be done using some properties of the participants, such as the maritime function or the sea basin covered. In this case, the CISE Node will request to the CISE Service Registry the definition of all the services compliant with these criteria.

The CISE Service Registry offers two services, FindService and GetServiceDetails, which are represented below.

Table 6: Service Discovery mechanisms

Service Name	Description	Input	Output
FindService	This service is invoked by the Adaptor to find services provided by participants.	Optional attributes: • Sea basin (ServiceProfile.SeaBasin) • Member State (ServiceProfile.Country) • Community (ServiceProfile.Community) • Function (ServiceProfile.Function) • Service type (Service.ServiceType) • Entities to exchange with optionallyspecific attributes (ServiceProfile.EntityTemplate) • Type of communication pattern (Service.ServiceOperation)	List of services with their characteristics using the following classes: • Service • Node • ServiceProfile • ServiceCapability • SubscriptionCapability (if the pattern is publish/subscribe)
GetServiceDetails	This service is invoked by the Adaptor if the entity service is already known to find out the service details, for instance the network parameters to address properly the message	Service ID (Service.ServiceID)	The service described by the following classes: • Service • Node • ServiceProfile • ServiceCapability • SubscriptionCapability (if the pattern is publish/subscribe)

The attribute ServiceProfile.EntityTemplate should be filled with an XSD message CISE Data Model [1]. This XSD message should give only the attributes needed or provided and the restrictions on some of the attributes (e.g. in case of list, the value supported).

6   The Service Types and Data Models

6.1   Introduction

The Service Type has a direct relation with the CISE Data Model ETSI GS CDM 005 [1] entities passed in the payload of the message.

Table 7 presents the list of Service Types and the corresponding supported entity types allowed.

The responsibility of the Adaptor is to ensure the correct setting of these fields and the Node will enforce these validations.

Each Service Type shall represent the access to a sub-tree of co-related Data Model entities, which should be strongly based on the subject of the Service Type (i.e. AnomalyType strongly correlates to anomaly-related data, and Anomaly is its **main** entity). Nonetheless, and due to the hierarchical representation of entities chosen for the Data Model (see ETSI GS CDM 003 [i.1]), a call for a given ServiceType may return other entities than the ones directly correlated to the ServiceType, as those would be presented as valid relationships at the moment of the call.

The possible relationships are defined in the CISE Data Model [1], and the Entities in Table 7 shall be supported.

Table 7: Service Types and main related Data Model entities

Service Type	Supported CISE Data Model entity
ActionService	Action
AgentService	Agent, Person, Organization, OrganizationalUnit, PortOrganization, FormalOrganization, OrganizationalCollaboration
AircraftService	Aircraft
AnomalyService	Anomaly
CargoDocumentService	CargoDocument
CargoService	Cargo, Catch, ContainementUnit
CertificateDocumentService	CertificateDocument
CrisisIncidentService	CrisisIncident
DocumentService	Document, VesselDocument, CargoDocument, EventDocument, LocationDocument, OrganizationDocument, RiskDocument, PersonDocument, CertificateDocument, Stream
EventDocumentService	EventDocument
IncidentService	Incident, MaritimeSafetyIncident, PollutionIncident, IrregularMigrationIncident, LawInfringementIncident, CrisisIncident
IrregularMigrationIncidentService	IrregularMigrationIncident
LandVehicleService	LandVehicle
LawInfringementIncidentService	LawInfringementIncident
LocationService	Location, PortLocation, PortFacilityLocation, NamedLocation
LocationDocumentService	LocationDocument
MaritimeSafetyIncidentService	MaritimeSafetyIncident, PollutionIncident
MeteoOceanographicConditionService	MeteoOceanographicCondition
MovementService	Movement
OperationalAssetService	OperationalAsset
OrganizationService	Organization, PortOrganization, OrganizationalUnit, OrganizationalCollaboration, FormalOrganization
OrganizationDocumentService	OrganizationDocument
PersonService	Person
PersonDocumentService	PersonDocument
RiskDocumentService	RiskDocument
RiskService	Risk
VesselDocumentService	VesselDocument
VesselService	Vessel

6.2 The Service Model Representation

The clauses below represent the Service Model entities relevant to the realization of information exchanges. Alongside each Service Model entity a class diagram is presented showing the direct relation with other entities. Not all the data structures herein described are intended to be used by Adaptors to send and receive messages. Some are used internally in the Node to Node communication protocols.

Clause 8 presents the message communication protocol with the expected Service Model data structures supported.

Clauses 6.3 to 6.7 below detail the data structures in each package, indicating:

- Entity name

- Entity description

- Fields Name

- Fields data type

- Fields description

- Fields concurrency. Where:

    - 0 .. 1 - Means the field is optional and at most has one occurrence.

    - 1 - Means the field is mandatory.

    - 0 .. N - Means the field is optional and could be a list of values.

    - 1 .. N - Means the field is mandatory and could be a list of values.
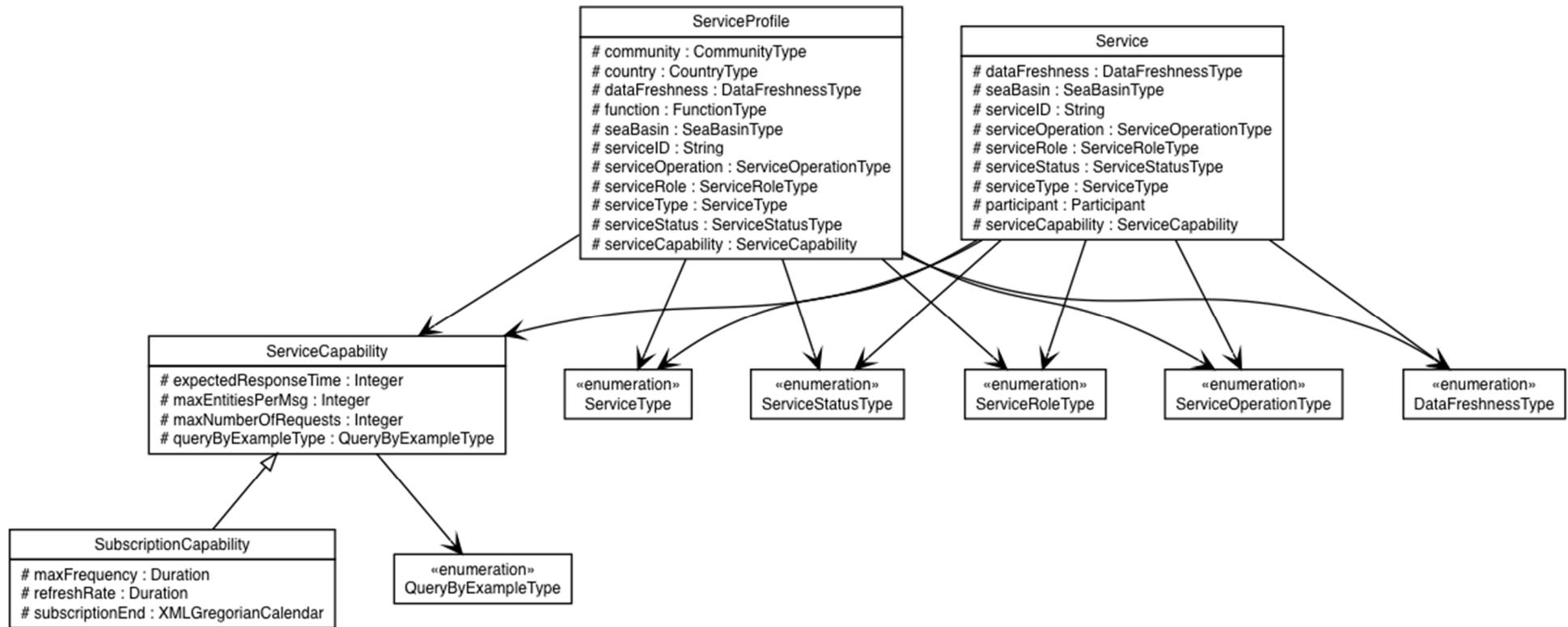
Figure 13: Service class diagram

6.3   Service

The Service entity contains the description of a service. See Figure 14 and Table 8 for the Service class description.

Message
eu.cise.servicemodel.v1.message

contextID : java.lang.String
correlationID : java.lang.String
creationDateTime : javax.xml.datatype.XMLGregorianCalendar
messageID : java.lang.String
priority : eu.cise.servicemodel.v1.message.PriorityType
requiresAck : java.lang.Boolean
sender : eu.cise.servicemodel.v1.service.Service
recipient : eu.cise.servicemodel.v1.service.Service
payload : eu.cise.servicemodel.v1.message.CoreEntityPayload
reliability : eu.cise.servicemodel.v1.message.ReliabilityProfile
ccRecipients : java.util.List<eu.cise.servicemodel.v1.service.Service>
any : org.w3c.dom.Element

Acknowledgement
eu.cise.servicemodel.v1.message

ackCode : eu.cise.servicemodel.v1.message.AcknowledgementType
ackDetail : java.lang.String
discoveredServices : java.util.List<eu.cise.servicemodel.v1.service.Service>

Service

dataFreshness : DataFreshnessType
seaBasin : SeaBasinType
serviceID : String
serviceOperation : ServiceOperationType
serviceRole : ServiceRoleType
serviceStatus : ServiceStatusType
serviceType : ServiceType
participant : Participant
serviceCapability : ServiceCapability

Participant
eu.cise.servicemodel.v1.authority

id : java.lang.String
name : java.lang.String
description : java.lang.String
classificationLevel : eu.cise.servicemodel.v1.authority.ClassificationLevelType
endpointUrl : java.lang.String
endpointType : eu.cise.servicemodel.v1.authority.EndpointType
providedServicesIds : java.util.List<java.lang.String>
gateway : eu.cise.servicemodel.v1.authority.Gateway
owner : java.lang.String
pointOfContact : eu.cise.servicemodel.v1.authority.PointOfContact
areasOfInterests : java.util.List<eu.cise.servicemodel.v1.authority.SeaBasinType>
communities : java.util.List<eu.cise.servicemodel.v1.authority.CommunityType>
functions : java.util.List<eu.cise.servicemodel.v1.authority.FunctionType>
memberState : eu.cise.servicemodel.v1.authority.CountryType

«enumeration»
ServiceType

«enumeration»
ServiceStatusType

«enumeration»
ServiceRoleType

«enumeration»
ServiceOperationType

ServiceCapability

expectedResponseTime : Integer
maxEntitiesPerMsg : Integer
maxNumberOfRequests : Integer
queryByExampleType : QueryByExampleType

«enumeration»
DataFreshnessType

«enumeration»
SeaBasinType
eu.cise.servicemodel.v1.authority

Figure 14: Service class diagram

Table 8: Service Class

Field Name	Data Type	Description	Occurs
DataFreshness	DataFreshnessType	This field specify what type of data is provided by the service. This is to distinguish real time data from historic data.	0..1
SeaBasin	SeaBasinType	The sea basin covered by the service.	0..1
ServiceID	String	This is the unique ID of the service.	1
ServiceOperation	ServiceOperationType	The type of communication pattern supported by the service (e.g. Pull/Push/Subscribe/Feedback).	1
ServiceRole	ServiceRoleType	Role of the service in the message exchange process (i.e. provider or consumer).	0..1
ServiceStatus	ServiceStatusType	The status of the service. Draft = the service is not yet available for use but can be seen in the Service Registry. Online = the service is available for use Maintenance = the service is temporally not available for use. Maintenance = The service is under maintenance, not available. Deprecated = the service is available for use but will be soon offline, either replaced by a new version of the service or discontinued. Offline = the service is not available anymore. For historic purpose, it can still be seen in the Service Registry with an offline status.	0..1
ServiceType	ServiceType	The service type gives the type of entities exchanged (based on the CISE data model).	0..1
Participant	Participant	Participant to which the service belongs.	0..1
ServiceCapability	ServiceCapability	The capabilities provided by the service.	0..1

6.4   ServiceCapability

This structure represents the different capabilities of a service. This can depend of the operation supported and will be further extended. See Figure 15 and Table 9.
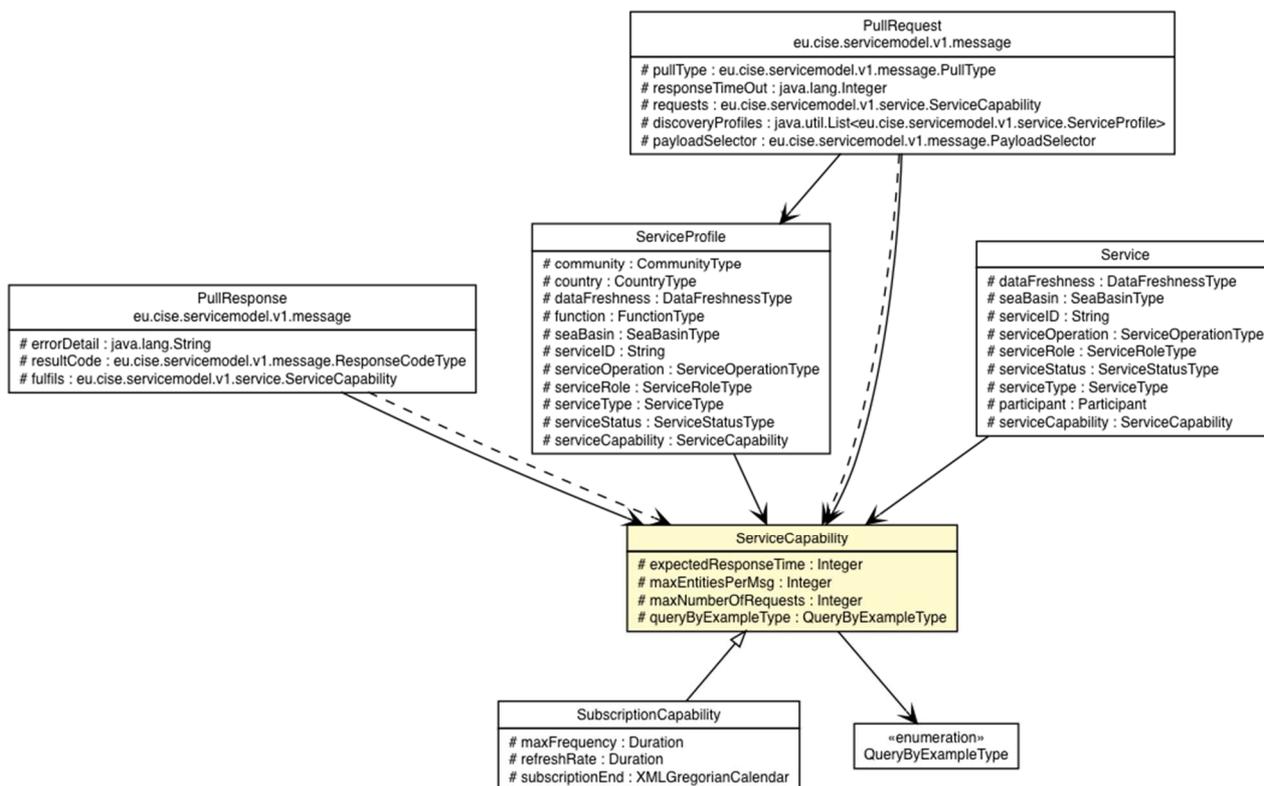
Figure 15: ServiceCapability class diagram

Table 9: Service Capability

Field Name	Data Type	Description	Occurs
MaxEntitiesPerMsg	Integer	Maximum number of entities returned in a pull response.	0..1
QueryByExampleType	QueryByExampleType	Type used for the query by example. This mechanism supports either exact answers or approximate answers.	0..1
ExpectedResponseTime	Integer	Estimated average time to receive a response.	0..1
MaxNumberOfRequests	Integer	Number of requests by hour allowed by the system providing. Undefined = no limit.	0..1

6.5   ServiceProfile

The ServiceProfile represents the characteristics associated to the service and to the provider of the Service. See Figure 16 and Table 10.
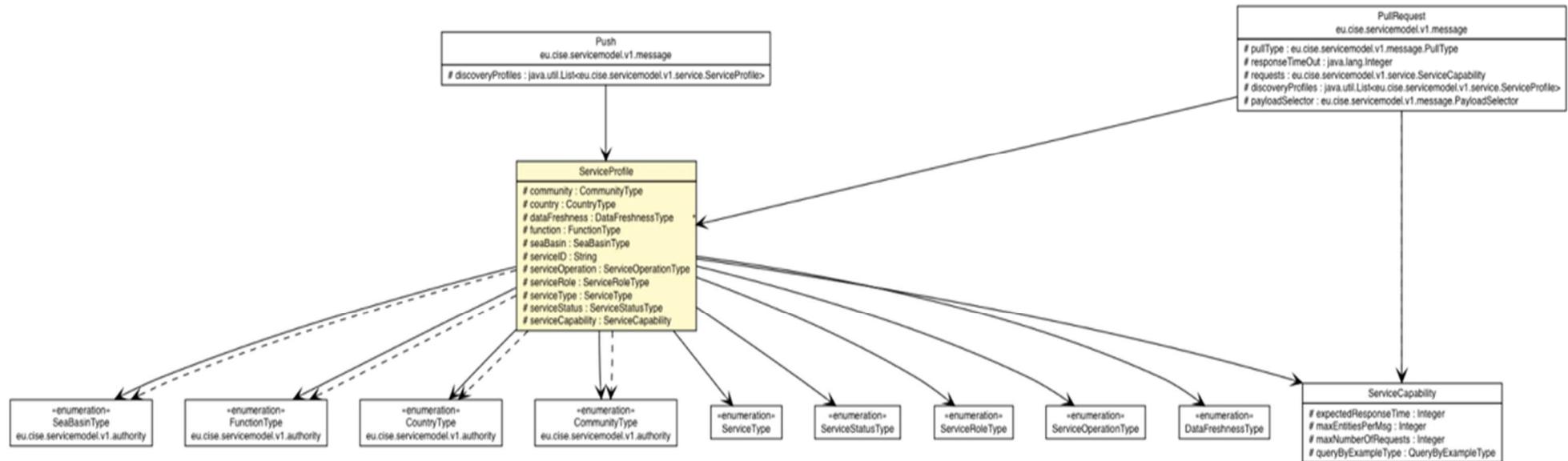
**Figure 16: ServiceProfile class diagram**

Table 10: Service Profile

Field Name	Data Type	Description	Occurs
Community	CommunityType	One of the 7 user communities participating to CISE. This field is related to the community of the provider of the service.	0..1
Country	CountryType	The Country of the provider of the service. The code ISO-3166-1 [2] alpha-2 is used: 2 character country code.	0..1
DataFreshness	DataFreshnessType	This field specify what type of data is provided by the service. This is to distinguish real time data from historic data.	0..1
Function	FunctionType	The function covered by the provider of the service.	0..1
SeaBasin	SeaBasinType	The sea basin covered by the service.	0..1
ServiceOperation	ServiceOperationType	Service operation type.	0..1
ServiceRole	ServiceRoleType	Service role.	0..1
ServiceID	String	Service unique identifier.	0..1
ServiceType	ServiceType	Service type.	0..1
ServiceStatus	ServiceStatusType	Service status.	0..1
ServiceCapability	ServiceCapability	Service capabilities.	0..1

6.6   SubscriptionCapability (extends ServiceCapability)

The SubscriptionCapability represents the capabilities specific for the subscribe pattern. See Figure 17 and Table 11.
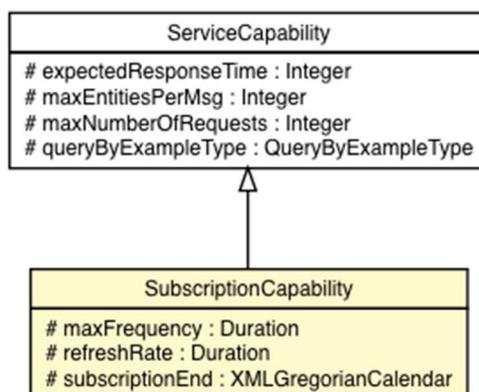
Figure 17: SubscriptionCapability class diagram

Table 11: Subscrition Capability

Field Name	Data Type	Description	Occurs
MaxFrequency	Duration	In the subscription pattern, the maximum frequency of update available. This information can be given for information by the service provider.	0..1
RefreshRate	Duration	In the subscription pattern, the average time between two updates. This information can be requested by the subscriber or given for information by the service provider.	0..1
SubscriptionEnd	dateTime	The date and time when the subscription should end. This information can be requested by the subscriber.	0..1

6.7   Accessory Enumerations

The following are support reference data enumerations in the CISE Service Model and, albeit not directly representing a root element in the protocol, are relevant for its completion.

Table 12: DataFreshnessType enumeration

Enumeration of the different type of data related to the time (real time or historic information)	
Value	**Description**
Historic	historic
RealTime	real time
NearlyRealTime	nearly real time
Unknown	Unknown

Table 13: QueryByExampleType enumeration

Enumeration of the different type of query	
Value	**Description**
BestEffort	best effort
ExactSearch	exact search

Table 14: ServiceOperationType enumeration

Enumeration of the different type of communication pattern available for each service type	
Value	**Description**
Pull	Pull operation
Push	Push operation
Subscribe	Subscribe operation
Acknowledgement	Acknowledgement operation
Feedback	Feedback operation

Table 15: ServiceRoleType enumeration

Role of the service in the message exchange process	
Value	**Description**
Consumer	If the service is able to receive information
Provider	If the service is able to provide information

Table 16: ServiceStatusType enumeration

| Enumeration of the different status of a service	
Value	**Description**
Draft	The service is available only to the provider
Online	The service is available to any CISE participant according to the access rights policy
Maintenance	The service is under maintenance, not available
Deprecated	This service is online and available for compatibility with previous versions of the specifications, but it can be removed in the next versions.
Offline	The service is registered but not available

Table 17: ServiceType enumeration

Enumeration of the different type of service related to the entity Data Model of CISE	
Value	**Description**
ActionService	This service exchanges the entity Action
AgentService	This service exchanges the entity Agent
AircraftService	This service exchanges the entity Aircraft
AnomalyService	This service exchanges the entity Anomaly
CargoDocumentService	This service exchanges the entity Document in relation to the entity Cargo
CargoService	This service exchanges the entity Cargo
CertificateDocumentService	This service exchanges the data objects of the CertificateDocument data entity
CrisisIncidentService	This service exchanges the entity CrisisIncident
DocumentService	This service exchanges the entity Document
EventDocumentService	This service exchanges the entity Document in relation to the entity Event
IncidentService	This service exchanges the entity Incident
IrregularMigration IncidentService	This service exchanges the entity IrregularMigrationIncident
LandVehicleService	This service exchanges the entity LandVehicle
LawInfringement IncidentService	This service exchanges the entity LawInfringementIncident
LocationService	This service exchanges the entity Location
LocationDocumentService	This service exchanges the data objects of the LocationDocument data entity
MaritimeSafety IncidentService	This service exchanges the entity MaritimeSafetyIncident
MeteoOceanographic ConditionService	This service exchanges the entity MeteoOceanographicCondition
MovementService	This service exchanges the entity Movement
OperationalAssetService	This service exchanges the entity OperationalAsset
OrganizationService	This service exchanges the entity Organization
OrganizationDocumentService	This service exchanges the data objects of the OrganizationDocument data entity
PersonService	This service exchanges the entity Person
PersonDocumentService	This service exchanges the data objects of the PersonDocument data entity
RiskDocumentService	This service exchanges the entity Document in relation to the entity Risk
RiskService	This service exchanges the entity Risk
VesselDocumentService	This service exchanges the data objects of the VesselDocument data entity
VesselService	This service exchanges the entity Vessel

7   The CISE Message Structure

7.1   Overview

In CISE, the Message class is an abstract entity, parent for Feedback, PullRequest, PullResponse, Push and Acknowledgment entities. These subtypes structures of the Message itself represent the operations and message exchange patterns available in CISE with the capability to transport the Data Model entity in their payload. These subtypes of Message in conjunction with the indication of the entity service type (e.g. VesselService, RiskService) cover all current services identified for CISE and allow an easier extension and flexibility for the future.

A simplified class model
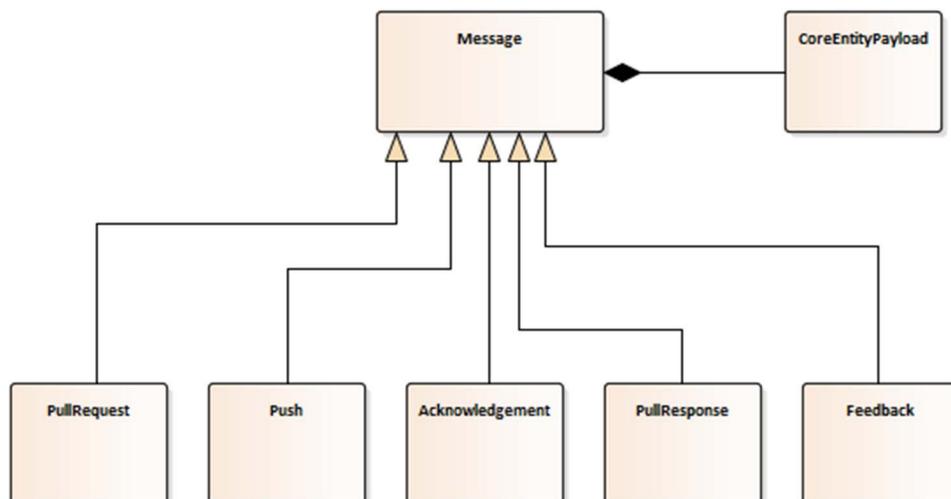
Figure 18: CISE Class Model

All communication protocols shall use specific message types (i.e. PullRequest, PullResponse, etc.) that extend the common Message class. In clause 7.2, the attributes of this root Message class are described.

7.2   The MESSAGE Package

7.2.1   Overview

The Message Package represents all Entities that deal with message passing in a CISE environment and their correlated supporting entities.
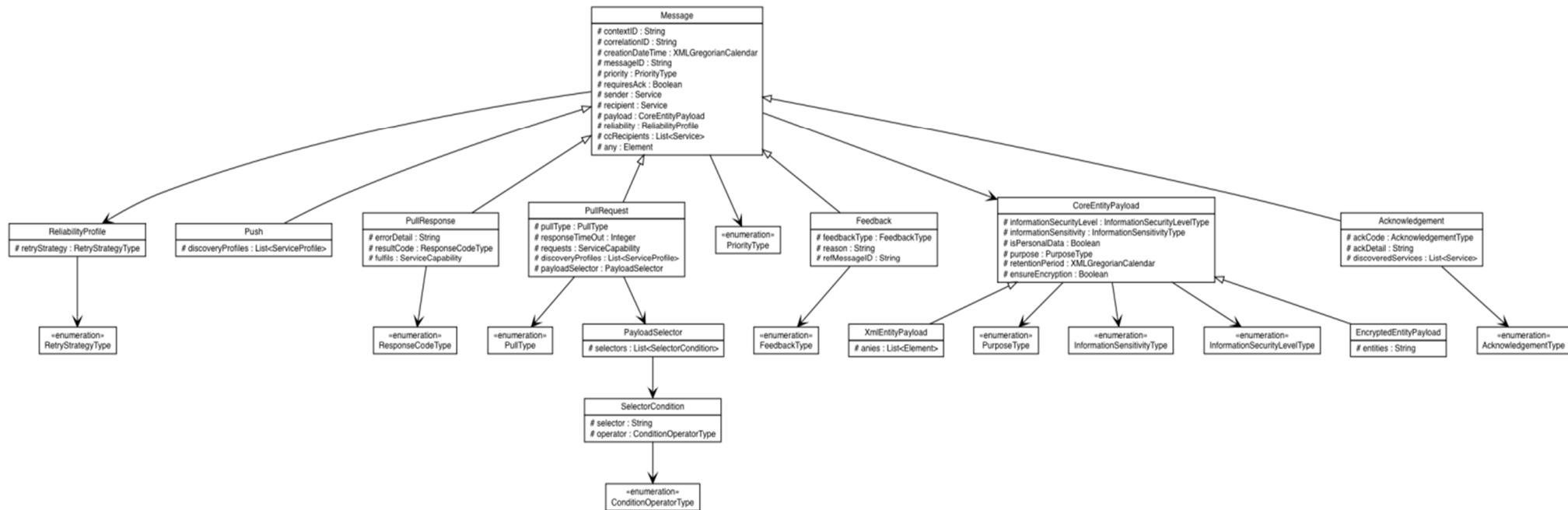
Figure 19: MESSAGE package class diagram

The base Message class have the attributes shown in Table 18.

Table 18: Message Class Attributes

Element	Required	Example Value	Description
MessageID	Yes	String of type UUID. Example: fd5b2bb2-8095-4acf-b6cb-3dd78ba8a572.	Identifier of the message. It is unique for the CISE participant who created the message.
CorrelationID	No	String of type UUID. Example: ad5b9bb2-6095-4xcf-b6cb-1dd78ba8a773.	This identifier correlates the request and response messages of/to a service (for the Pull or the Publish/Subscribe communication patterns). In other words, when create a response message, value this attribute with the original MessageID.
ContextID	No	String of type UUID	This identifier correlates the messages that share an operational need. For instance, in order to update the information of an incident, several CISE entity services need to be invoked (e.g. IncidentService, EventLocationService, etc.). Thus, the messages exchanged with these CISE entity services are related by this ID type.
Priority	Yes	One of the different priority of a message: • Low • Medium • High	Priority of the message, to help the receiver of the message to deal with prioritizing the messages received.
RequiresAck	No	Boolean	Indication that Sender wants to receive an asynchronous Acknowledgement upon delivery of this message in the final destination.
Sender	Yes	Participant	This field describes the sender of the message.
Recipient	No	Participant	This field describes the recipient of the message.
Payload	No	CoreEntityPayload	This entity contains the business payload of the message and the metadata related to this payload. This is used by all messages types expect the Acknowledgement type.
Reliability	No	Allowed values: • LowReliability • HighReliability • NoRetry	This entity contains information about the retry strategy in case of error during the transmission of the message.
CcRecipients	No	Participant	Other recipients that also received this message. Can be repeated unlimited.

7.2.2   PullRequest (extends Message)

The Pull Request is used in the Pull communication pattern to request information**.**
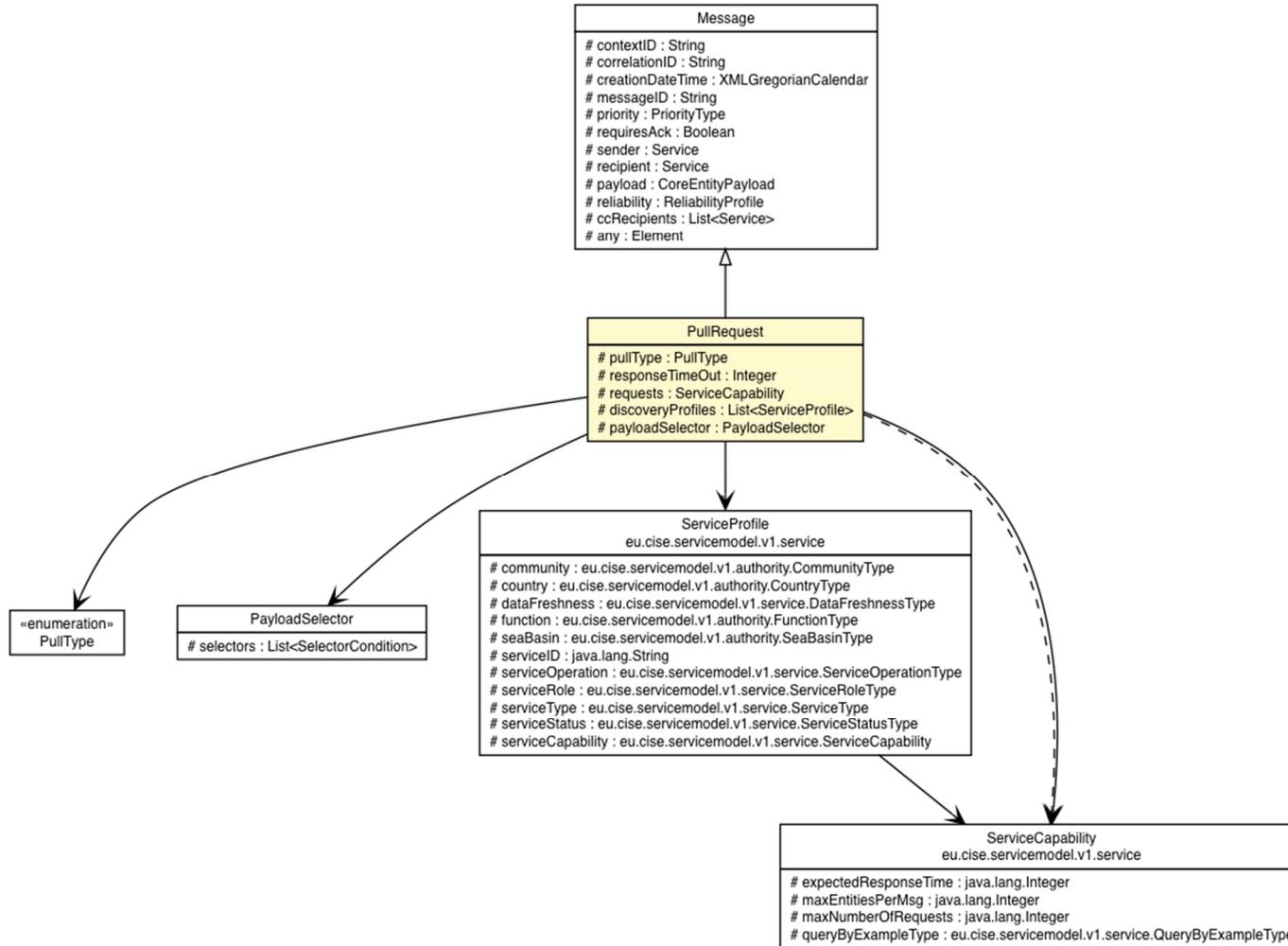
Figure 20: PullRequest class diagram

Table 19: Pull Request class fields

Field Name	Data Type	Description	Occurs
PullType	PullType	The Pull Type is to distinguish between the simple request and the subscription mechanism. It can also be used to unsubscribe to a flow.	1
ResponseTimeOut	Integer	Time in seconds. The request should be answered within this time limit. After this time, the response may not be considered by the requesting system.	0..1
Requests	ServiceCapability	Service Capability required by the system requesting the information. This will indicate for instance the maximum entities expected in return.	0..1
DiscoveryProfiles	ServiceProfile	This field is used for the Legacy System to request the CISE Node to look for services of a specific type and/or from a specific type of provider (e.g. using the community, country or sea basin...).	0..1
PayloadSelector	PayloadSelector	Filters to be considered on the message payload entities when using a Pull Request.	0..1

7.2.3　PullResponse (extends Message)

The Pull Response is used in the Pull communication pattern to respond to a request. This response is sent asynchronously.
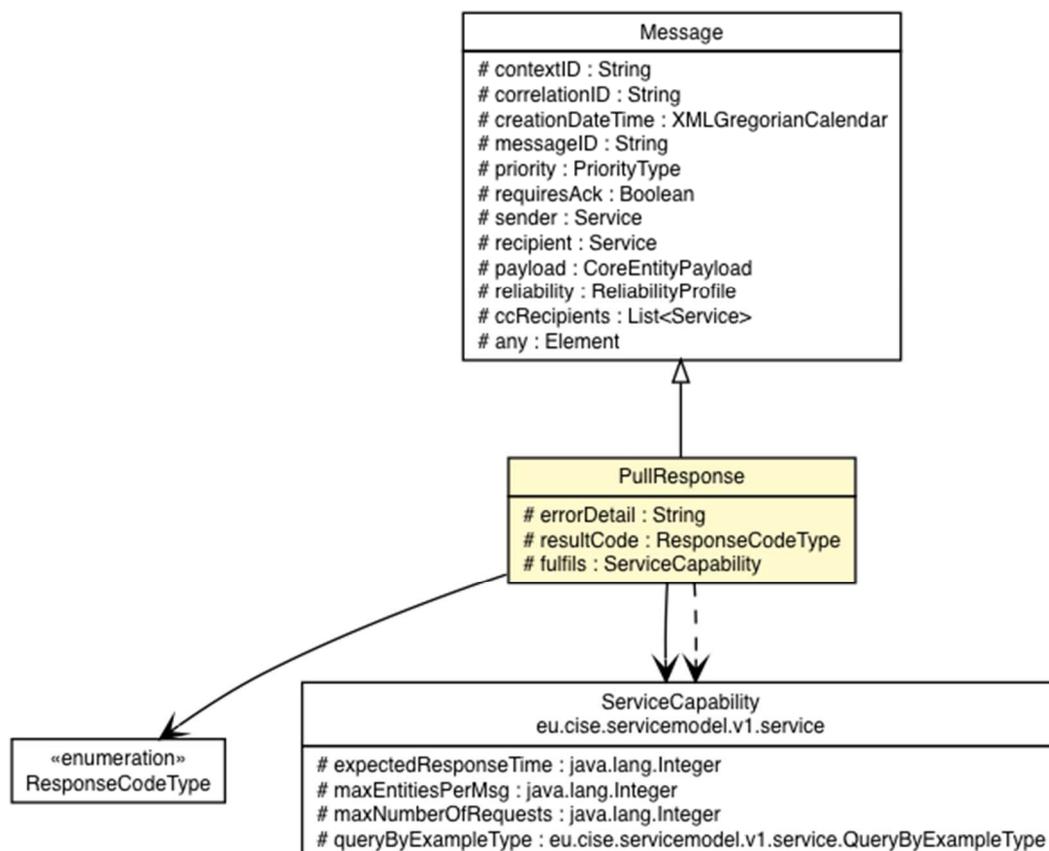

Figure 21: PullResponse class diagram

Table 20: PullResponse class fields

Field Name	Data Type	Description	Occurs
ErrorDetail	String	This field may give a textual description of an error that could have happened during the process of the pull request message. This can be used to communicate an error that happened after sending the acknowledgement message.	0..1
ResultCode	ResponseCodeType	This field provides an OK code if the response is sent along with the pull response. It can also provide an error code if an error occurred after sending the acknowledgement message.	1
Fulfils	ServiceCapability	Describes the characteristics used to respond to the request. For instance, the type of query performed (exact or best effort).	0..1

7.2.4   Push (extends Message)

The Push is used in the Push communication pattern to transmit information to other CISE participants.
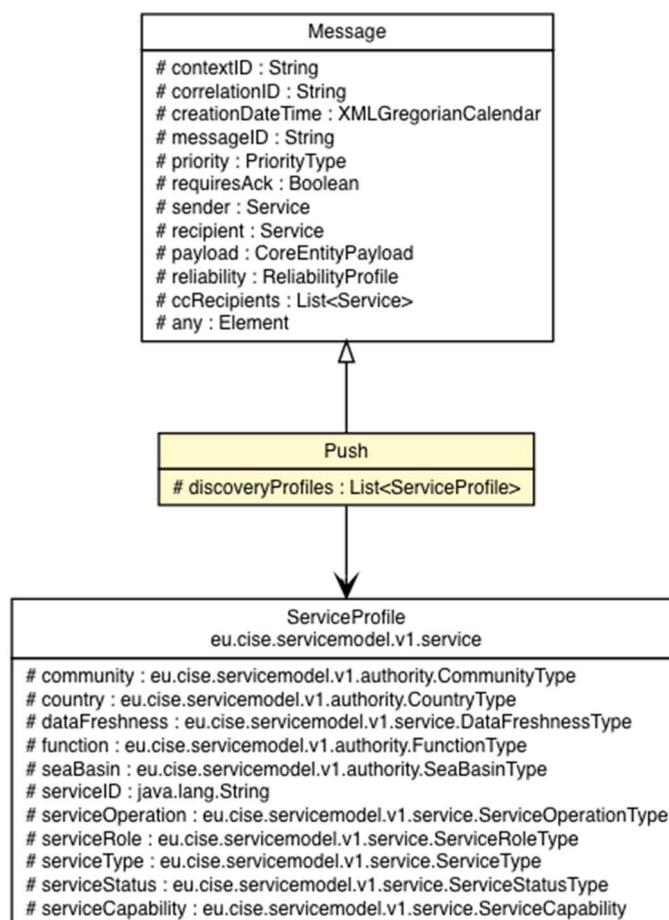
Figure 22: Push class diagram

Table 21: Push class fields

Field Name	Data Type	Description	Occurs
DiscoveryProfiles	ServiceProfile	This field is used for the Legacy System to request the CISE Node to look for services of a specific type and/or from a specific type of provider (e.g. using the community, country or sea basin, ...).	0..N

7.2.5   Acknowledgement (extends Message)

The Acknowledgement message is used in two distinct situations:

- As a synchronous message: the web service operation return and represents the acknowledgment that the message has been received by the sending Node.

- It is sent asynchronously by the destination Nodes, with the status of the delivery to the final message recipient if required by the senders. It might be also used to handle retry mechanisms.
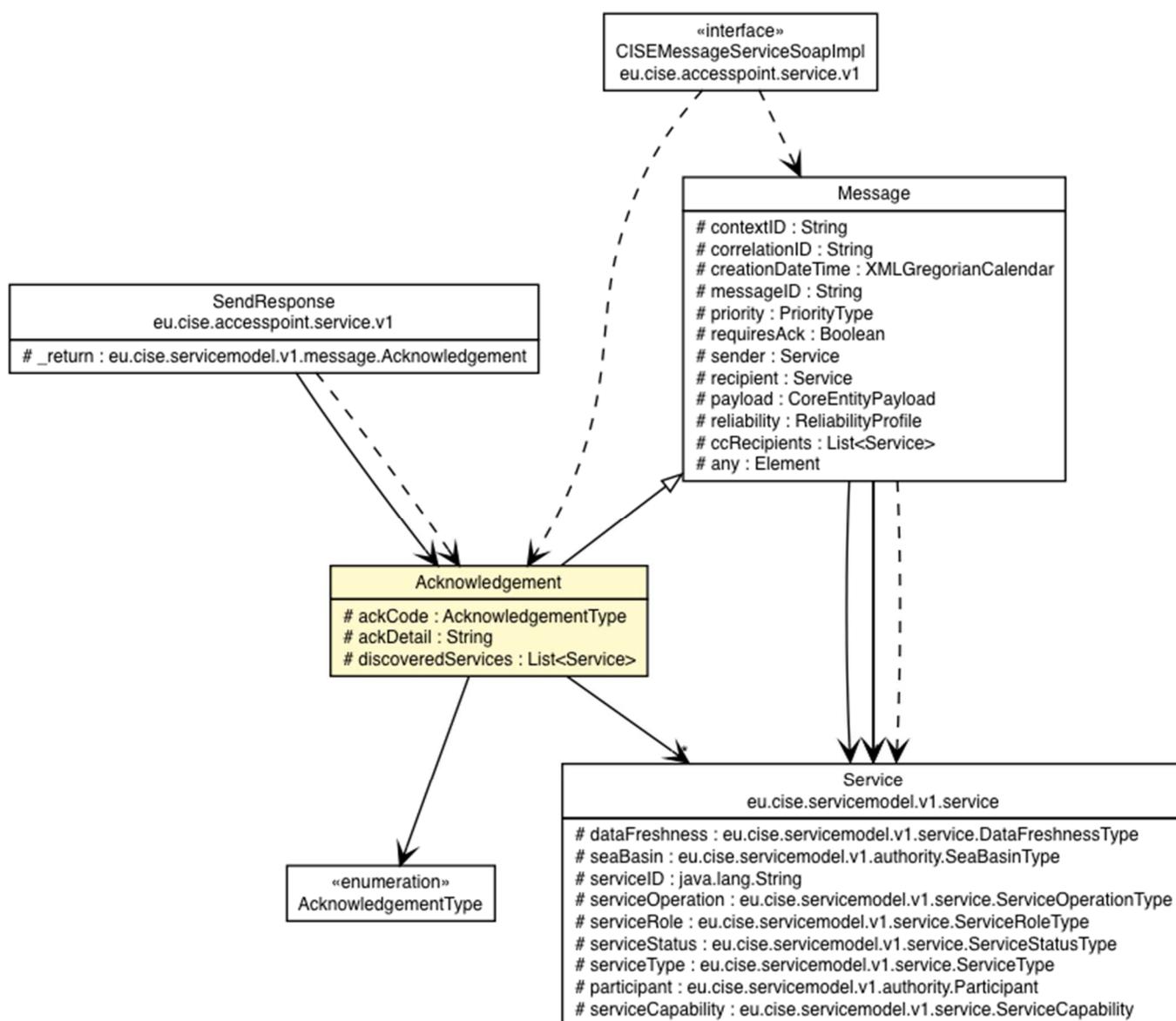
Figure 23: Acknowledgement class diagram

Table 22: Acknowledge class fields

Field Name	Data Type	Description	Occurs
AckCode	AcknowledgementType	This code represents the type of fault that occurred, or an indication of success.	1
AckDetail	String	Additional text to clarify details about the fault.	0..1
DiscoveredServices	Service	Used in operations like to Discovery or Get Subscribers to return the results of the operation, in the synchronous acknowledgement.	0..N

7.2.6 Feedback (extends Message)

This message type allows to provide feedback on a message already sent (for example when a message was sent by error) or on a message received.
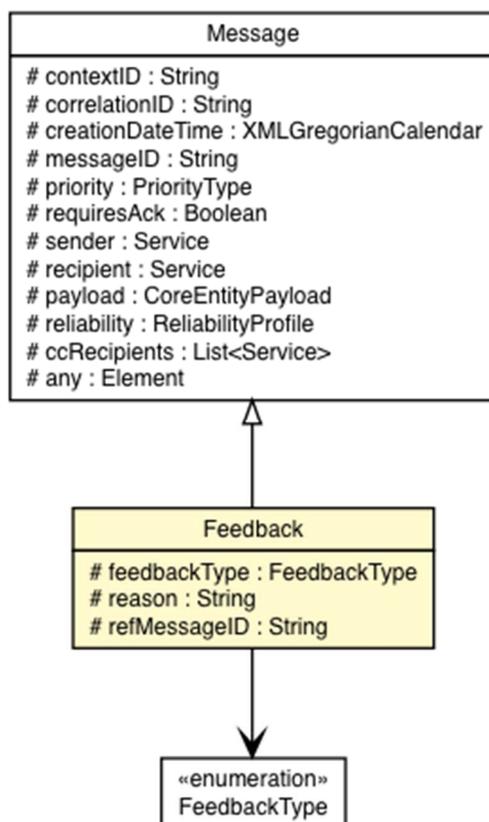
Figure 24: Feedback class diagram

Table 23: Feedback class fields

Field Name	Data Type	Description	Occurs
FeedbackType	FeedbackType	The type of feedback to provide.	1
Reason	String	The description of the reason for feedback. This field is a free text.	0..1
RefMessageID	String	The Message ID that this feedback message refers to.	1

7.3 The AUTHORITY Package

7.3.1 Overview

The AUTHORITY Package describes the participants and correlated Entities representing the interactions agents that participate in a CISE Network.
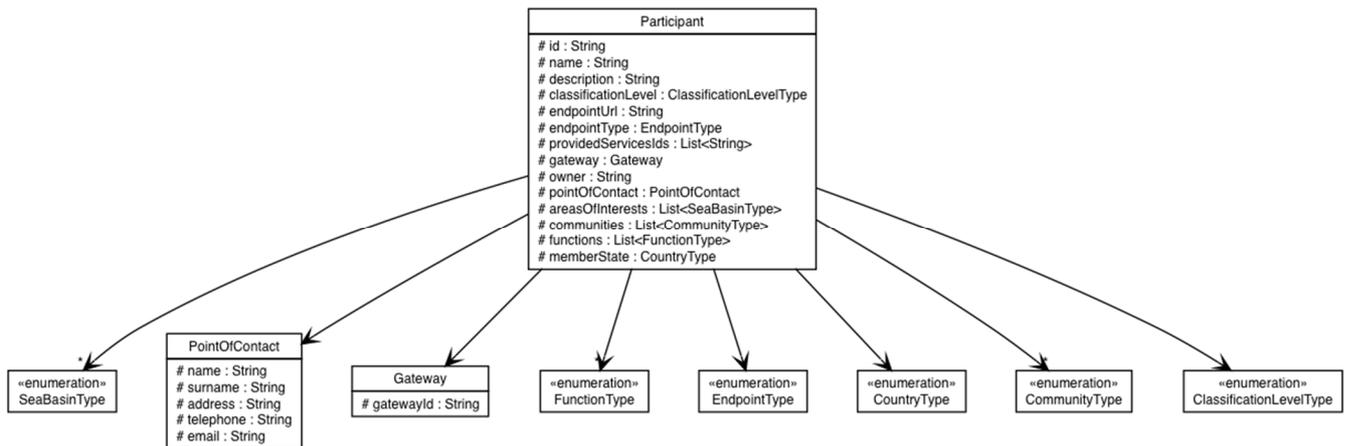
Figure 25: AUTHORITY package class diagram

7.3.2   Gateway (Node)

The Gateway structure represents the Node providing the service. This entity provides the information required for routing the messages between nodes.
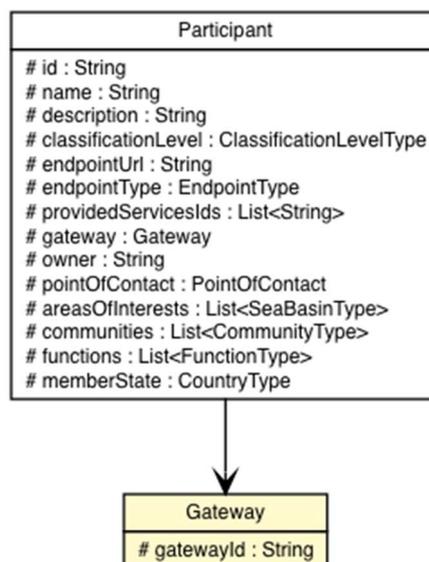
Figure 26: Node class diagram

Table 24: Gateway class fields

| Field Name	Data Type	Description	Occurs
GatewayId	String	The unique identifier of the Node.	1

7.3.3   Participant

A Participant system connecting to a CISE network.

Service
eu.cise.servicemodel.v1.service

dataFreshness : eu.cise.servicemodel.v1.service.DataFreshnessType
seaBasin : eu.cise.servicemodel.v1.authority.SeaBasinType
serviceID : java.lang.String
serviceOperation : eu.cise.servicemodel.v1.service.ServiceOperationType
serviceRole : eu.cise.servicemodel.v1.service.ServiceRoleType
serviceStatus : eu.cise.servicemodel.v1.service.ServiceStatusType
serviceType : eu.cise.servicemodel.v1.service.ServiceType
participant : eu.cise.servicemodel.v1.authority.Participant
serviceCapability : eu.cise.servicemodel.v1.service.ServiceCapability

Participant

id : String
name : String
description : String
classificationLevel : ClassificationLevelType
endpointUrl : String
endpointType : EndpointType
providedServicesIds : List<String>
gateway : Gateway
owner : String
pointOfContact : PointOfContact
areasOfInterests : List<SeaBasinType>
communities : List<CommunityType>
functions : List<FunctionType>
memberState : CountryType

«enumeration»
SeaBasinType

PointOfContact
name : String
surname : String
address : String
telephone : String
email : String

Gateway
gatewayId : String

«enumeration»
FunctionType

«enumeration»
EndpointType

«enumeration»
CountryType

«enumeration»
CommunityType

«enumeration»
ClassificationLevelType

Figure 27: Participant class diagram

Table 25: Participant Class fields

Field Name	Data Type	Description	Occurs
Id	String	Unique identifier of the Participant	0..1
Name	String	Name of the Participant	0..1
Description	String	Full description of the Participant	0..1
ClassificationLevel	ClassificationLevelType	Unclassified or EURestricted	0..1
EndpointType	EndpointType	Rest or Soap	0..1
EndpointUrl	String	Endpoint Url	0..1
ProvidedServicesId	String	List of the services provided by the Participant	0..N
Node	Node	Node where the Legacy System is connected to	0..1
Owner	String	The Authority that owns the Legacy System	0..1
PointOfContact	PointOfContact	Point of contact information	0..1
AreasOfInterest	SeaBasinType	List of areas of interest	0..N
Communities	CommunityType	One of the user communities participating to CISE. This field is related to the community of the provider of the service.	0..N
Functions	FunctionType	The functions covered by the participant providing the service.	0..N
MemberState	CountryType	The Country of the provider of the service. The code ISO-3166-1 alpha-2 is used: 2 character country code. --Example "FR" for France.	0..1

7.3.4   PointOfContact

This Entity represents the Point of contact of a Participant.
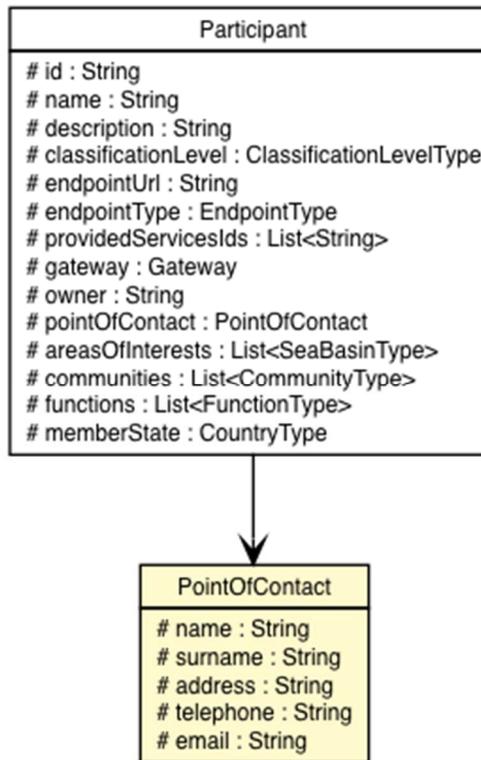
Figure 28: PointOfContact class diagram

Table 26: Point of Contact class fields

Field Name	Data Type	Description	Occurs
Address	String	Address of the Point of Contact	0..1
E-Mail	String	Email of the Point of Contact	0..1
Name	String	Name of the Point of Contact	0..1
Surname	String	Surname of the Point of Contact	0..1
Telephone	String	Phone Number of the Point of Contact	0..1

7.3.6   CoreEntityPayload

This abstract entity contains the business payload of the message and the metadata related to this payload. This is used by all messages types expect the Acknowledgement type.

Message

\# contextID : String
\# correlationID : String
\# creationDateTime : XMLGregorianCalendar
\# messageID : String
\# priority : PriorityType
\# requiresAck : Boolean
\# sender : Service
\# recipient : Service
\# payload : CoreEntityPayload
\# reliability : ReliabilityProfile
\# ccRecipients : List<Service>
\# any : Element

CoreEntityPayload

\# informationSecurityLevel : InformationSecurityLevelType
\# informationSensitivity : InformationSensitivityType
\# isPersonalData : Boolean
\# purpose : PurposeType
\# retentionPeriod : XMLGregorianCalendar
\# ensureEncryption : Boolean

XmlEntityPayload

\# anies : List<Element>

«enumeration»
PurposeType

«enumeration»
InformationSensitivityType

«enumeration»
InformationSecurityLevelType

EncryptedEntityPayload

\# entities : String

Figure 29: CoreEntityPayload class diagram

Table 27: Core Entity class fields

Field Name	Data Type	Description	Occurs
InformationSecurityLevel	InformationSecurityLevelType	Level of security associated with the payload.	1
InformationSensitivity	InformationSensitivityType	Level of sensitivity related to the payload.	1
IsPersonalData	Boolean	If the payload contains personal data.	0..1
Purpose	PurposeType	The purpose of the message. It can be used to handle access rights on the provider side.	1
RetentionPeriod	dateTime	Date and Time until when the payload can be kept. This information can be used for the legal constraints associated with the management of personal data.	0..1
EnsureEncryption	Boolean	An indication the payload is encrypted.	0..1

7.3.7   EncryptedEntityPayload (extends CoreEntityPayload)

The EncryptedEntityPayload is a Sub entity used to transfer the encrypted payload information. The encryption method, cypher keys, algorithms, etc., have to be previously agreed and exchange between the participants sending and receiving the message.
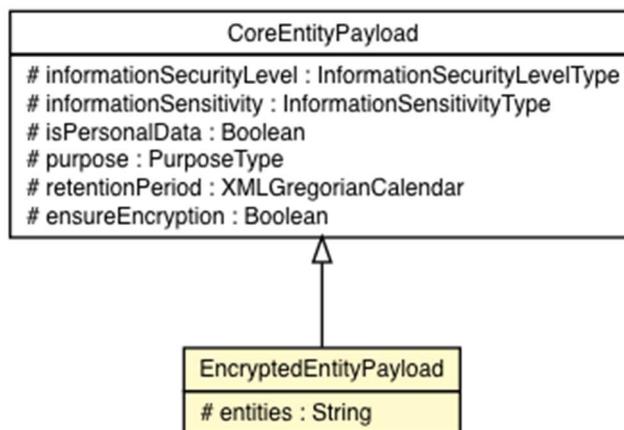
Figure 30: EncryptedEntityPayload class diagram

Table 28: Entities class fields

Field Name	Data Type	Description	Occurs
Entities	String	Encrypted data encoded in BASE64 format.	1

7.3.8   PayloadSelector

The PayloadSelector specifies Filters to be considered on the message payload entities when using a Pull Request.
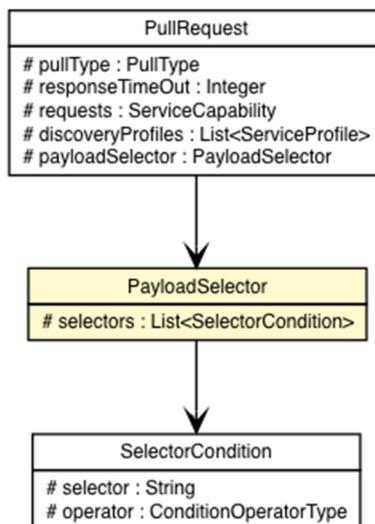
Figure 31: PayloadSelector class diagram

Table 29: Payload Selector class fields

Filters to be considered on the message payload entities when using a Pull Request			
Field Name	**Data Type**	**Description**	**Occurs**
Selectors	SelectorCondition	List of selector conditions.	1..N

7.3.9   ReliabilityProfile

This entity contains information about the retry strategy in case of error during the transmission of the message.
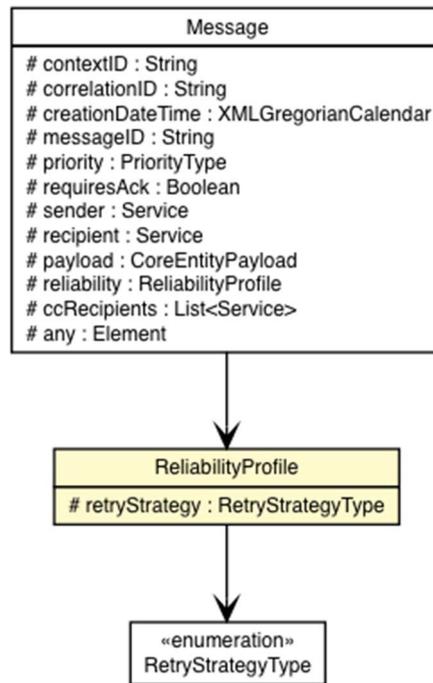
Figure 32: ReliabilityProfile class diagram

Table 30: Reliability Profile

Field Name	Data Type	Description	Occurs
RetryStrategy	RetryStrategyType	The type of retry strategy required by this message. For each type, a retry mechanism has been agreed at EU level (e.g. number of retry, time between each try...). This mechanism is implemented by the CISE Nodes.	1

7.3.10   SelectorCondition (extends PayloadSelector)

This Entity represents a condition to be used to allow addition extra filtering on data.
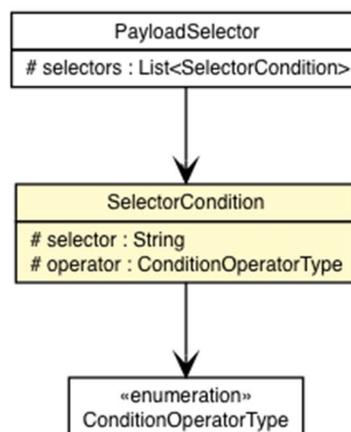
Figure 33: SelectorCondition class diagram

Table 31: Selector

Field Name	Data Type	Description	Occurs
Selector	String	XPATH expression that allows the selection XML elements in the payload.	1
Operator	ConditionOperatorType	Operator to be applied to this selector.	1

7.3.11   XmlEntityPayload (extends CoreEntityPayload)

This is a sub entity used to transfer CISE Data Model entities as XML Elements.
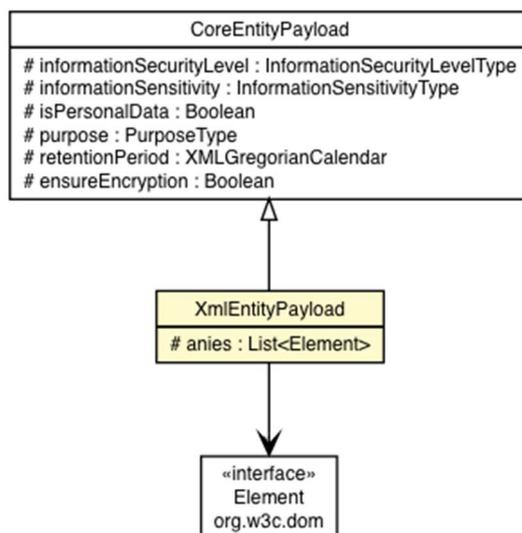
Figure 34: XmlEntityPayload class diagram

Table 32: Xml Entity Payload

Sub entity used to transfer CISE Data Model entities.			
Field Name	**Data Type**	**Description**	**Occurs**
Entities	XML Element	The list of entities transmitted in the message. This refers to the CISE data model. The content of this field will be checked with the data model XML Schema.	0..N

7.3.12   Accessory Enumerations

The following are support reference data enumerations in the CISE Service Model and, albeit not directly representing a root element in the protocol, are relevant for its completion.

Table 33: ClassificationLevelType enumeration

Enumeration with the classification levels for the transferred data	
Value	**Description**
Unclassified	Unclassified
EURestricted	EURestricted

Table 34: CommunityType enumeration

Enumeration of the different communities that can belong a CISE participant	
Value	**Description**
GeneralLawEnforcement	General Law Enforcement
Customs	Customs
MarineEnvironment	Marine Environment
MaritimeSafetySecurity	Maritime Safety and Security
DefenceMonitoring	Defence
FisheriesControl	Fisheries control
BorderControl	Border control
Other	Other
NonSpecified	Non-specified

Table 35: AcknowledgementType enumeration

Enumeration with the several types of Acknowledgment codes that can be written	
Value	**Description**
Success	Success
EndPointNotFound	End point not found
SecurityError	Security error
InternalGatewayFault	Internal Node fault
InvalidRequestObject	Invalid request object
Unauthorized	Unauthorized error
BadRequest	Bad request
ServiceTypeNotSupported	Service type not supported
EntityTypeNotAccepted	Entity type not accepted
ObjectTypeNotAccepted	Object type not accepted
ServerError	Server error
TimestampError	Timestamp error
AuthenticationError	Authentication error
NetworkError	Network error
ServiceManagerError	Service Manager error

Table 36: ConditionOperatorType enumeration

Enumeration with the types of operators that can be used in payload selectors	
Value	**Description**
EQUAL	Equal
NOT_EQUAL	Not equal
LIKE	Similar to usage to SQL 92 LIKE operator where is assumed the usage of the percentage (%) symbol inside the value to compare.
NOT_LIKE	Similar to usage to SQL 92 LIKE operator where is assumed the usage of the percentage (%) symbol inside the value to compare.
IS_NULL	Is null
GREATER_THAN	Greater Than
GREATER_THAN_OR_EQUAL_TO	Greater Than Or Equal To
LESS_THAN	Less Than
LESS_THAN_OR_EQUAL_TO	Less Than Or Equal To

Table 37: FeedbackType enumeration

Enumeration of the type of feedback for the feedback message	
Value	**Description**
info	Information on a previous message
delete	Request for deleting a previous message

Table 38: InformationSecurityLevelType enumeration

This enumeration presents the possible values for information security classification. The enumeration is based in the security rules for protecting EU classified.	
Value	**Description**
EUTopSecret	Information and material the unauthorized disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.
EUSecret	Information and material the unauthorized disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.
EUConfidential	Information and material the unauthorized disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.
EURestricted	Information and material the unauthorized disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.
NonClassified	It can be used for information and material whose classification level is still pending.
NonSpecified	It can be used for information and material whose classification level is not specified.

Table 39: InformationSensitivityType enumeration

This enumeration presents the possible values for information sensitivity degree. The Traffic Light Protocol (TLP) of US-CERT is applied.	
Value	**Description**
Red	TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.
Amber	TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
Green	TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
White	TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
NonSpecified	It can be used for information and material whose classification level is not specified.

Table 40: PriorityType enumeration

Enumeration of the different priority of a message	
Value	**Description**
Low	Low priority message.
Medium	Medium priority message.
High	High priority message.

Table 41: PullType enumeration

Enumeration to handle the different type of Pull Request message	
Value	**Description**
GetSubscribers	Operation to get the list of subscribers for the service.
Discover	Operation to discover services.
Request	Operation to request data.
Subscribe	Operation to subscribe for services.
Unsubscribe	Operation to unsubscribe for services.

7.3.13   EndpointType (enumeration)

The full list of values can be consulted in the supplied XSD zip file, contained in archive gs_cdm004v01000p0.zip which accompanies the present document.

It is based on Alpha-2 ISO 3166-1 [2] country codes.

Table 42: EndpointType enumeration

Enumeration with the list of available CISE service interface protocols	
Value	Description
REST	REST service interface
SOAP	SOAP service interface

Table 43: FunctionType enumeration

Enumeration of the different functions covered by a CISE participant	
Value	Description
VTM	Vessel traffic management
Safety	Vessel Traffic Safety
Security	Monitoring of security of ships
SAR	Search and Rescue
Operation	Support of response and enforcement operations (anti-piracy, SAR, salvage)
FisheriesWarning	Early warning of illegal fisheries or fish landings
FisheriesMonitoring	Monitoring of compliance with regulations on fisheries
FisheriesOperation	Support of response and enforcement operations
EnvironmentMonitoring	Monitoring of compliance with regulations
EnvironmentWarning	Early warning of environmental accidents and incidents
EnvironmentResponse	Support of pollution response operations
CustomsMonitoring	Monitoring of compliance with customs regulation on import, export and movement of goods
Customs Operation	Support of enforcement operations
BorderMonitoring	Monitoring of compliance with regulations on immigration and border control crossings
BorderOperation	Support of enforcement operations
LawEnforcementMonitoring	Monitoring of compliance with applicable legislation in sea areas where police competence is required
LawEnforcementOperation	Support to enforcement and response operations
DefenceMonitoring	Monitoring in support of defence tasks such as national sovereignty at sea
CounterTerrorism	Combatting terrorism and other hostile activities outside the EU
CSDPTask	Other CSDP tasks as defined in Articles 42 and 43 TEU
NonSpecified	Non-specified

Table 44: SeaBasinType enumeration

Enumeration of the different European Sea Basins	
Value	Description
Atlantic	Atlantic
BalticSea	Baltic Sea
NorthSea	North Sea
Mediterranean	Mediterranean
BlackSea	Black Sea
OutermostRegions	Outermost Regions
ArcticOcean	Arctic Ocean
NonSpecified	Non-specified

Table 45: PurposeType enumeration

Enumeration of the different purpose linked to a request	
Value	**Description**
VTM	Vessel Traffic Management
Safety	Vessel Traffic Safety
Security	Monitoring of security of ships
SAR	Search and Rescue
Operation	Support of response and enforcement operations (anti-piracy, SAR, salvage).
FisheriesWarning	Early warning of illegal fisheries or fish landings
FisheriesMonitoring	Monitoring of compliance with regulations on fisheries
FisheriesOperation	Support of response and enforcement operations
EnvironmentMonitoring	Monitoring of compliance with regulations
EnvironmentWarning	Early warning of environmental accidents and incidents
EnvironmentResponse	Support of pollution response operations
CustomsMonitoring	Monitoring of compliance with customs regulation on import, export and movement of goods
CustomsOperation	Support of enforcement operations
BorderMonitoring	Monitoring of compliance with regulations on immigration and border control crossings
BorderOperation	Support of enforcement operations
LawEnforcementMonitoring	Monitoring of compliance with applicable legislation in sea areas where police competence is required
LawEnforcementOperation	Support to enforcement and response operations
DefenceMonitoring	Monitoring in support of defence tasks such as national sovereignty at sea
CounterTerrorism	Combatting terrorism and other hostile activities outside the EU
CSDPTask	Other CSDP tasks as defined in Articles and TEU
NonSpecified	Non-specified

Table 46: ResponseCodeType enumeration

Enumeration with the code values return with a PullResponse	
Value	**Description**
Success	Success
EndPointNotFound	End point not found
SecurityError	Security error
InternalGatewayFault	Internal Node fault
InvalidRequestObject	Invalid request object
Unauthorized	Unauthorized error
BadRequest	Bad request
ServiceTypeNotSupported	Service type not supported
EntityTypeNotAccepted	Entity type not accepted
ObjectTypeNotAccepted	Object type not accepted
ServerError	Server error
TimestampError	Timestamp error
AuthenticationError	Authentication error

Table 47: RetryStrategyType enumeration

Enumeration of the different type of retry strategy	
Value	**Description**
NoRetry	no retry
LowReliabilty	low reliabilty
HighReliability	high reliability

8   The CISE Communication Flows

8.1   Communication Protocol and Supported Operations

8.1.1   Overview

The Service Model allows several business operations that use the message exchange patterns defined for CISE. It is through these operations that Legacy Systems/Adaptors send and receive information, always using the previously defined Service (and single Entity-operation).

All available operations are supported by a set of data structures that make the CISE Service Model. At the base there is the previously described abstract Message structure which is extended in the sub entities Push, Pull Request, Pull Response, Feedback and Acknowledgement (Figure 35).
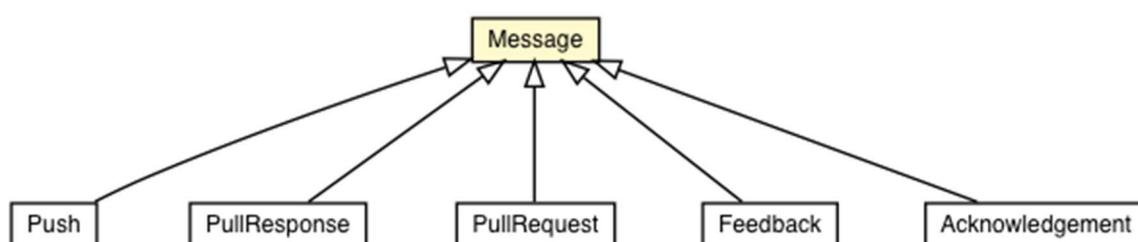
Figure 35: Message and sub entities

These five data structures are the core messages that allow the operations described in the clauses below.

Full data structures definition and descriptions is supplied in the form of XSD's and in the file "CDM004_Service_Model_XSDs_v1.0.zip" contained in archive gs_cdm004v01000p0.zip which accompanies the present document. The clauses below present the message communication protocol with the expected Service Model data structures supported in each of the envisaged operations.

8.1.2   Push

The push operation is used to notify other participants regarding information they subscribed or are willing to receive.
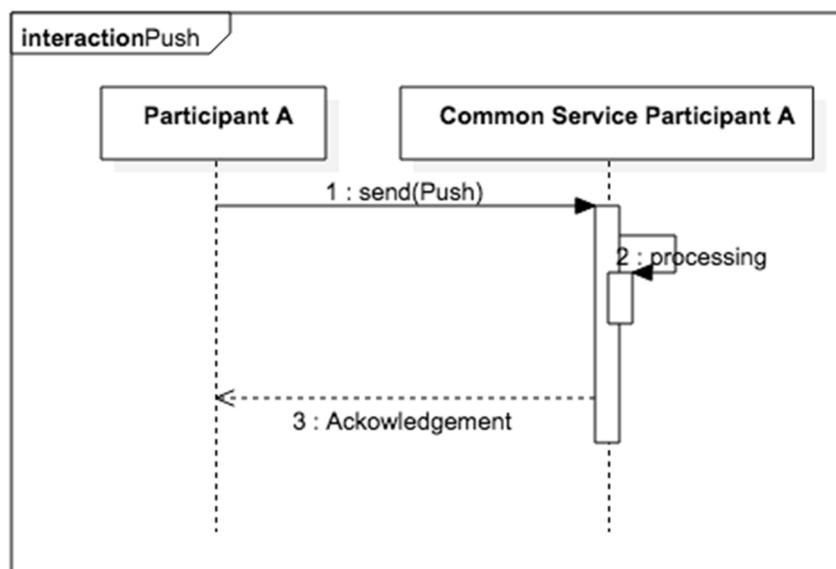
Figure 36: Common Services Push operation

In this operation, the provider Adaptor shall send a Push message and receive an Acknowledgement indicating that the message has been sent to the CISE network (its consumers). This Acknowledgement is a sub entity of Message and should not be confused with any other type of acknowledgement that might be transparently used in lower API levels, like HTTP or TCP.
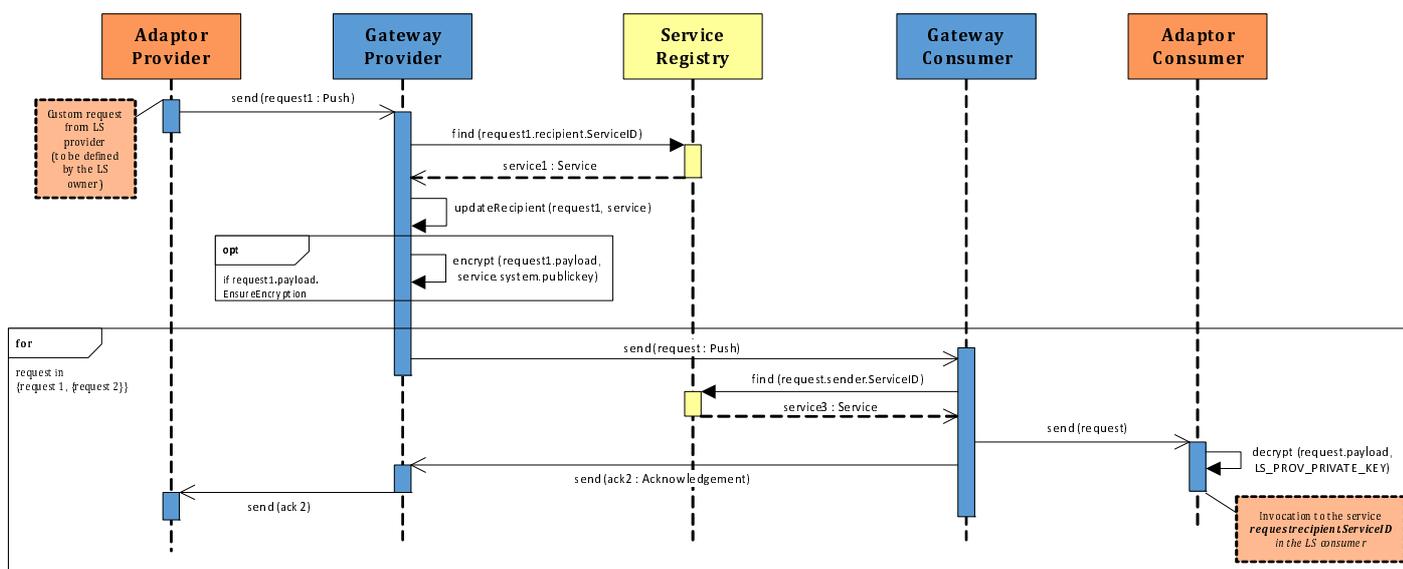
Figure 37: Push (to a known consumer)

Whenever the recipient is known to the sender, it should be set in the message, but if not set by the Adaptor then the Node will try to discover possible recipients based on the discovery profiles information present in the message. This last case is also known as "Push to unknown".

In the case of this operation, the Adaptor might use before the operation GetSubscribers to find out which services have subscribed to its information and then send a message for each known recipient.

8.1.3   Pull (Request/Response)

The Pull Request and Pull Response operations happen in two different moments in time; since the pull operation is asynchronous, its results will arrive later in the form of a Pull Response.
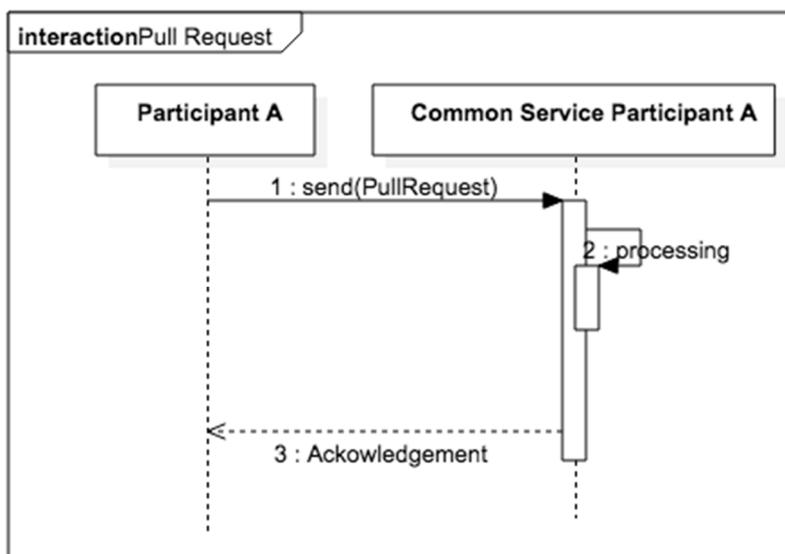
Figure 38: Common Services pull request operation

The consumer Adaptor will send a Pull Request message and receive an Acknowledgement indicating that the message has been sent to the CISE network.

Depending on the value of the field "requiresAck" (if value "true") other asynchronous Acknowledgements might be received later indicating that the message has been delivered to the destination Adaptor.

Later in time the destination Adaptors that received the Pull Request will prepare a response and send a Pull Response message to the requestor.
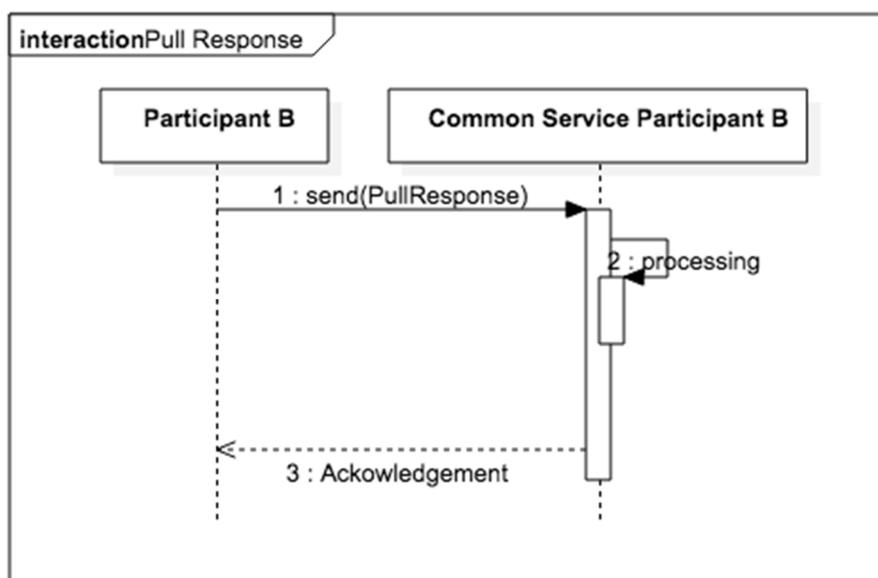
Figure 39: Common Services pull response operation

A detailed flow is shown in Figure 40 and Figure 41 below.
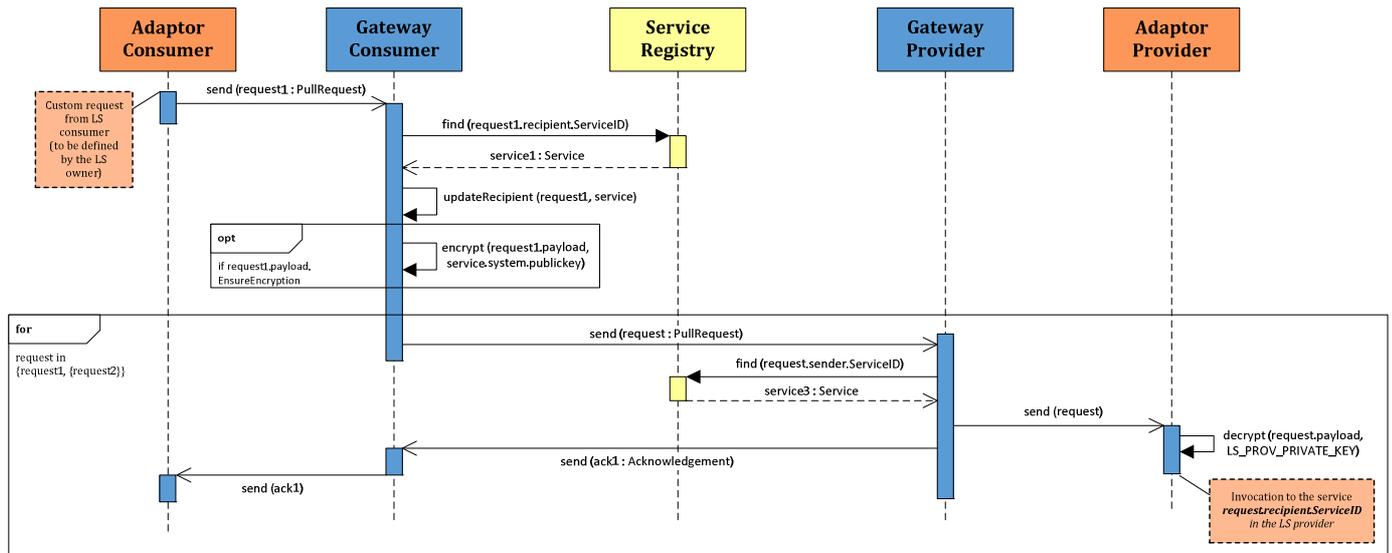
Figure 40: PullRequest (to a known provider)
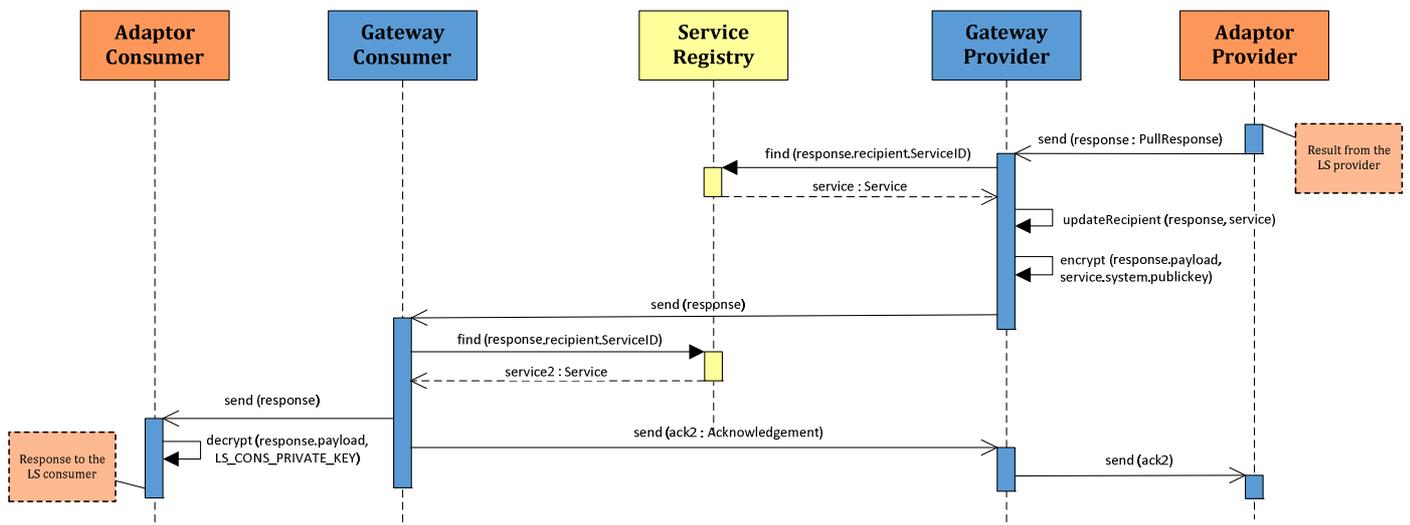
Figure 41: PullResponse from the provider

8.1.4 Pull Request Querying Mechanism

A request to a CISE provider can search for all the data entities that are similar to a given example (e.g. an input template).

It lays on the principles of the Query By Example pattern but adds semantic control to the adaptor, enabling it to have more operations on the selected query fields.

For a given CISE service one can query by its main entity, e.g. the VesselService will accept queries on Vessels and on any sub related entity, VesselInLocation for instance.

The description of a query in Query By Example is achieved by assigning values to the elements that one wants to filter. For instance, when searching for all vessels with name Mary, the service payload should be a Vessel type with the name attribute filled with "Mary".

One can easily spot that this approach is rather limitative once it only covers the scenario for an absolute match filter type. In order to provide a richer filter declaration, widely spread in any query language, some functionalities were added to allow the usage of more filter operators.

The following operators were devised:

- For numeric and dates: Greater Than, Greater Than or Equal, Less Than, Less Than or Equal

- For Text: StartsWith, EndsWith, Contains

- For Enumerations: Different

By default, the operator is always equal, meaning that, if no selection is made to a given attribute then the operator to apply in such filter is the equal operation.

In order to allow the intersection between filters, the entity should be repeated, the logical operation to apply in such repetitions is always the logical AND.

The following examples instantiate the conjunction of different operators.

1) Vessels that weight between 4 700 and 47 000 Ton.

```
<ns3:PullRequestType>
    <...>
    <Payload>
        <Vessel>
            <NetTonnage>4700.0</NetTonnage>
        </Vessel>
        <Vessel>
            <NetTonnage>47000.0</NetTonnage>
        </Vessel>
    </Payload>
            < PayloadSelector >
                < Selectors >
                    <Selector>//Vessel[1]/NetTonnage</Selector>
                    <Operator>GREATER_THAN</Operator>
                </ Selectors >
                < Selectors >
                    <Selector>//Vessel[2]/NetTonnage</Selector>
                    <Operator>LESS_THAN_OR_EQUAL_TO</Operator>
                </ Selectors >
            </ PayloadSelector >
</ns3:PullRequestType>
```

2) Vessels which have name starting with Queen and ends with II, for instance Queen Mary II.

```
<ns3:PullRequestType>
    <...>
    <Payload>
        <Vessel>
            <Name>Queen%</Name>
        </Vessel>
        <Vessel>
```

```
            <Name>%II</Name>
        </Vessel>
    </Payload>
            < PayloadSelector >
                < Selectors >
                    <Selector>//Vessel[0]/Name</Selector>
                    <Operator>LIKE</Operator>
                </ Selectors >
                < Selectors >
                    <Selector>//Vessel[1]/Name</Selector>
                    <Operator>LIKE</Operator>
                </ Selectors >
            </ PayloadSelector >
</ns3:PullRequestType>
```

3)   Ships that have a CargoType different than NoCargoUnitLiquidBulkGoods and NoCargoUnitSolidBulkGoods.

```
<ns3:PullRequestType>
    <...>
    <Payload>
        <Vessel>
            <CargoType>NoCargoUnitLiquidBulkGoods</CargoType>
        </Vessel>
        <Vessel>
            <CargoType>NoCargoUnitSolidBulkGoods</CargoType>
        </Vessel>
    </Payload>
            < PayloadSelector >
                < Selectors >
                    <Selector>//Vessel[0]/CargoType</Selector>
                    <Operator>NOT_EQUAL</Operator>
                </ Selectors >
                < Selectors >
                    <Selector>//Vessel[1]/CargoType</Selector>
                    <Operator>NOT_EQUAL</Operator>
                </ Selectors >
            </ PayloadSelector >
</ns3:PullRequestType>
```

Having in consideration that legacy systems will not support some kinds of filtering, the query originator system shall specify a degree of satisfaction or conformity to the applied criteria, stating if such criteria is very strict (each criterion has to be met) or if, on the other hand, a more lenient criteria could be applied in case the target system could not fully implement all filters in the criteria.

One of two level of completeness identifiers (Best Effort and Exact Match) shall be specified by the query originator.

When Best Effort is specified, the target system shall fulfil at least one of the filters, and if it cannot fulfil at least one, an error shall be returned.

When an Exact Match is specified all the filters shall be implemented, and if one is not implemented the target system shall return an error.

8.1.5   Pull (Request/Response)

The sending of feedback is triggered by a Participant willing to send additional information regarding a previous sent or received message.
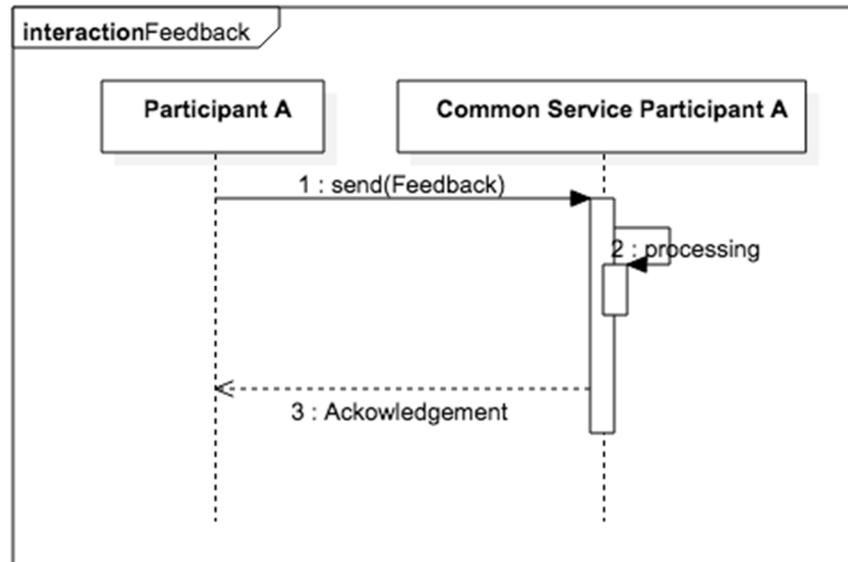
Figure 42: Common Services feedback operation

A detailed flow is shown in Figure 43 below.
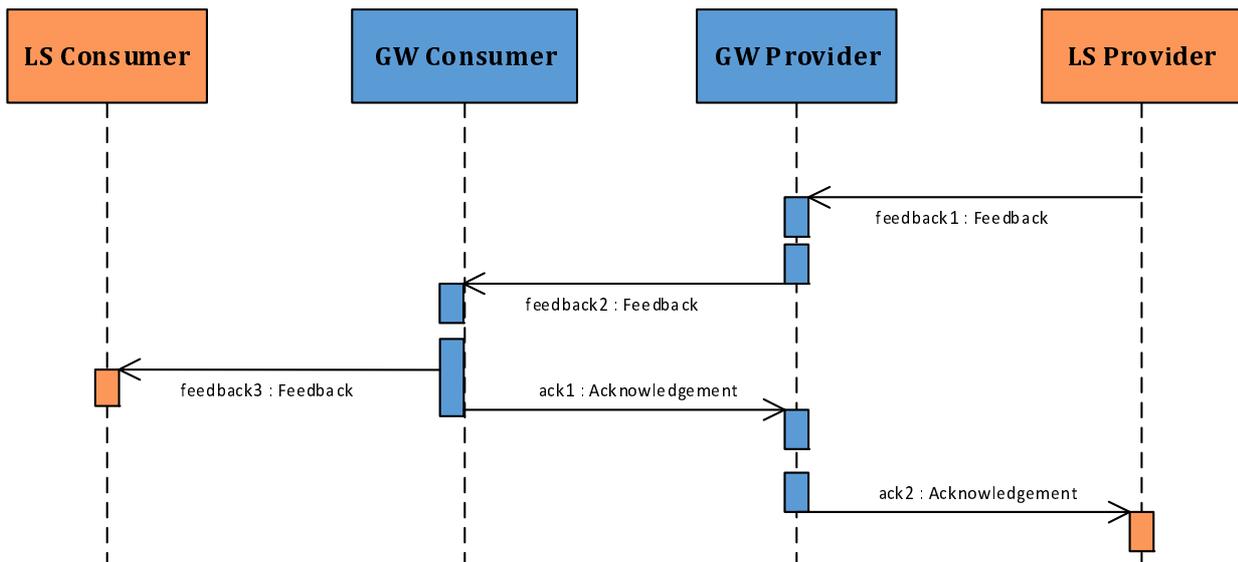
Figure 43: Common Services flow

8.1.6   Publish/Subscribe

The Publish/Subscribe pattern consists of three independent communication processes: one for subscription (handled with the Pull operation), one to cancel the subscription and another for publication (handled with the Push operation).
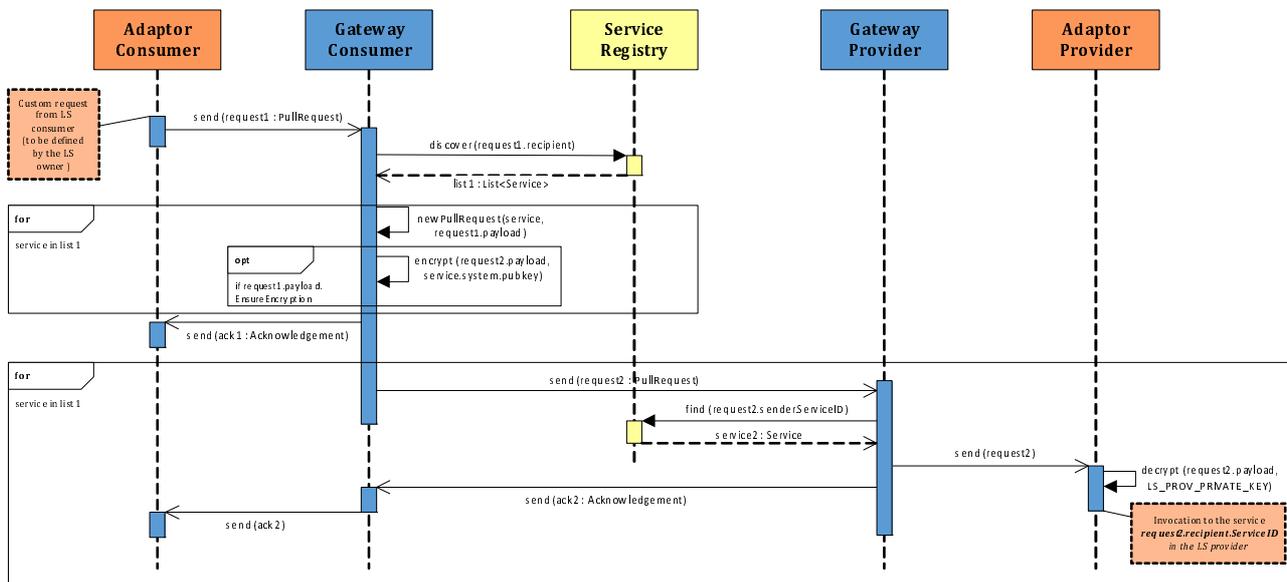
Figure 44: PullRequest (to unknown provider)

- Subscribe: the CISE consumer subscribes to a piece of information of the CISE provider using the Pull operation. In this case, the PullRequest message should indicate that it is a subscription process (PullType = subscribe).
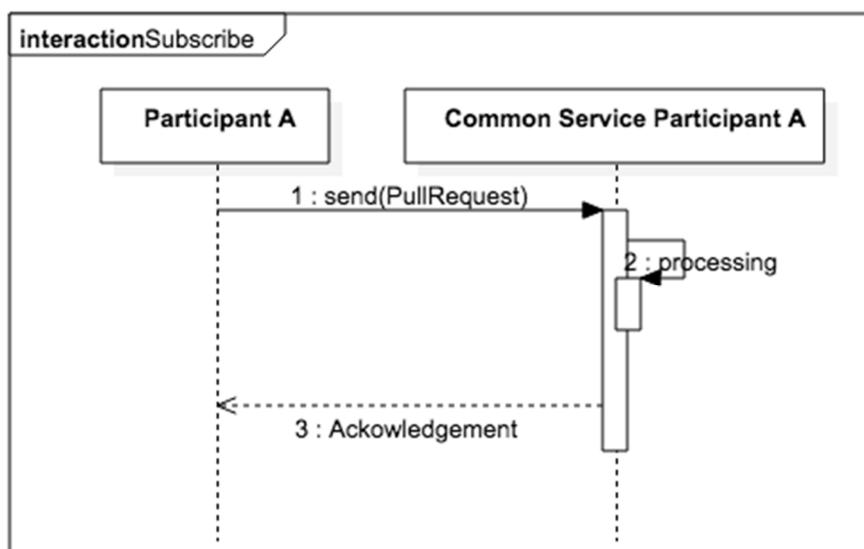
Figure 45: Common Services subscribe operation

- Publish: When the CISE provider wants to make available information (e.g. a list of data objects), the provider has two possibilities:

    - Either it first checks the list of subscribers (CISE consumers) with the GetSubscribers operation, and, subsequently, to each subscriber, the provider sends a Push message with the correlation ID received in the subscription operation.

-       Or, it delegates the responsibility of finding out the subscribers to the Node. In this case the provider will send just one message (a Push with ServiceOperation='Subscribe') without setting the recipients. The Node, upon receiving the message, will query the internal database where all subscribers are stored, sending to each subscriber a copy of the original message (generating a new message id and setting the recipient).
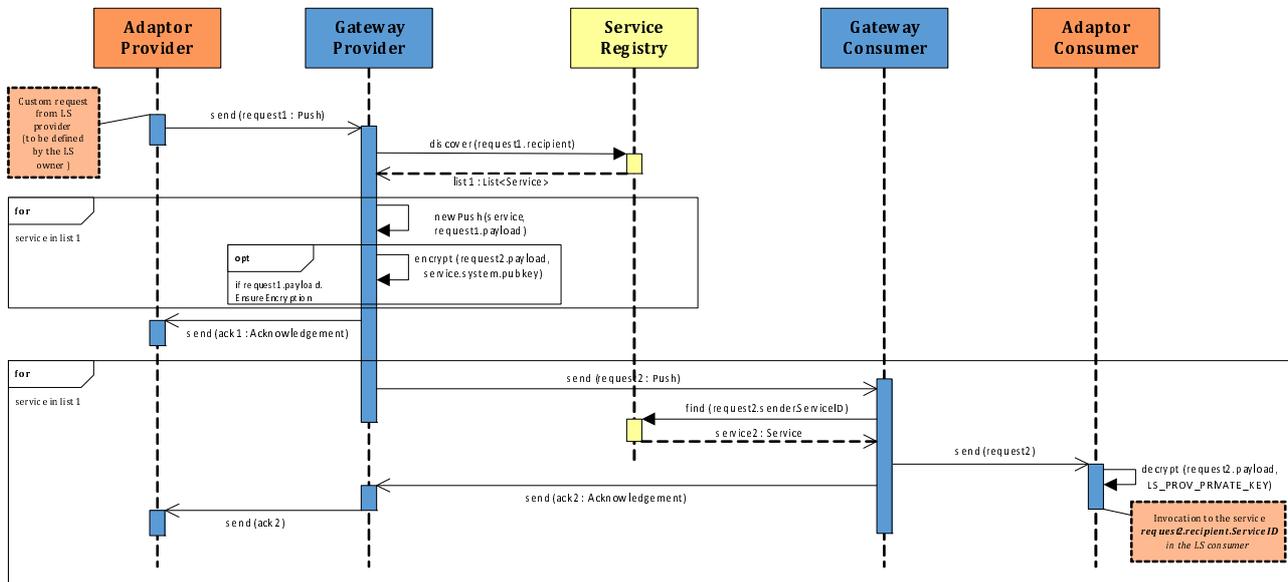

Figure 46: Common Services publish flow

- **Unsubscribe.** The subscription can last for a time period given in the SubscriptionCapability parameter (SubscriptionEnd) or until the CISE consumer unsubscribes using the PullRequest message (PullType = unsubscribe).
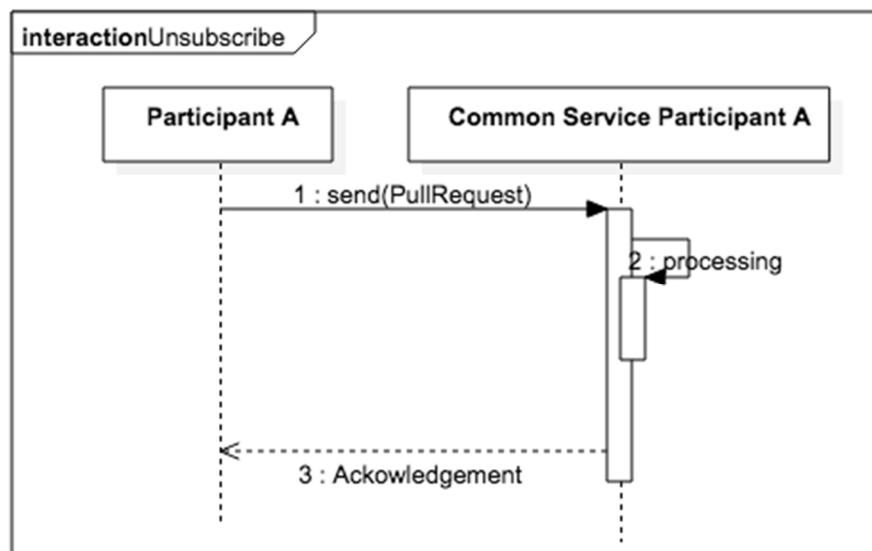
Figure 47: Common Services unsubscribe operation

8.1.7   Discover

The discover operation shall be used by a participant to find out other participant systems that supply information services with the pretended profile.

Since this operation is executed only between the Adaptor and its Node, the operation is synchronous in the sense that the Adaptor shall send a Pull Request message of indicating in the pull type "Discover", and shall receive in the Acknowledgment the eventual discovered services.
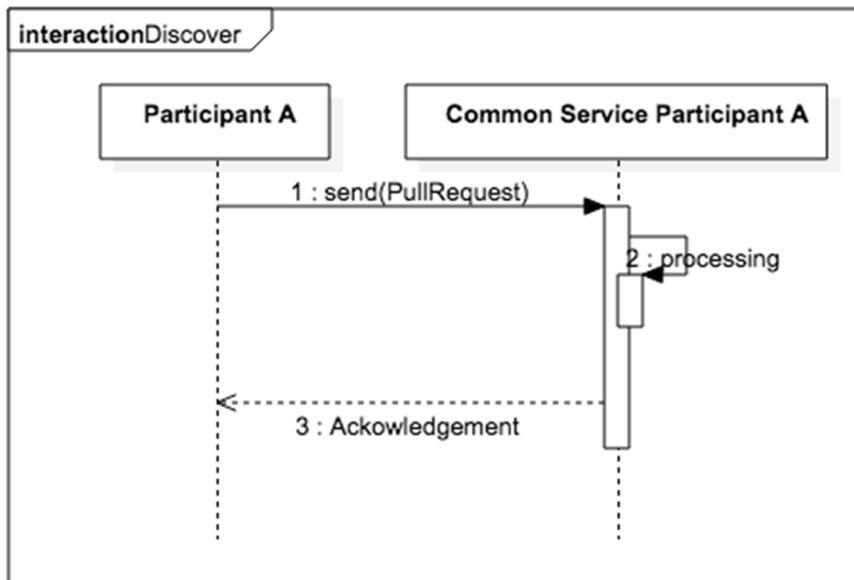

Figure 48: Common Services discover operation

8.1.8   Get Subscribers

A participant may request the list of recipients that have previously subscribed to its services.

The Adaptor shall send a Pull Request message indicating in the pull type "Get Subscribers" and will receive in the Acknowledgment the eventual subscribed services.

In this operation, the return (Acknowledgment) has a different purpose than in other cases because it will return also the values of the operation.
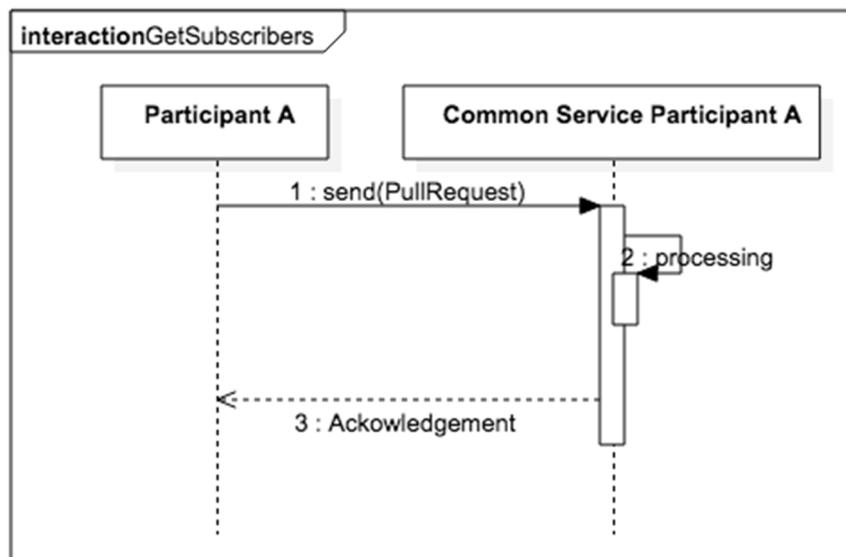
Figure 49: Common Services get subscribers operation

8.1.9   Asynchronous Acknowledgment

An asynchronous Acknowledgment shall be sent by the recipients Node upon successful or unsuccessful delivery of a message to the Adaptor.

The sending of this message should only be performed if the sender explicitly marks the field "requiresAck" as "true" in the sent message (Pull Request, Pull Response, Feedback, Push).

The diagram in Figure 50 demonstrates the sequence of steps, in this case for a Pull Request but equal to other types of messages except the Acknowledgment itself. The Acknowledgment message is the only message type outside of this asynchronous acknowledgment to avoid recursive Acknowledgement messages being sent thus potentially generating an infinite cycle.
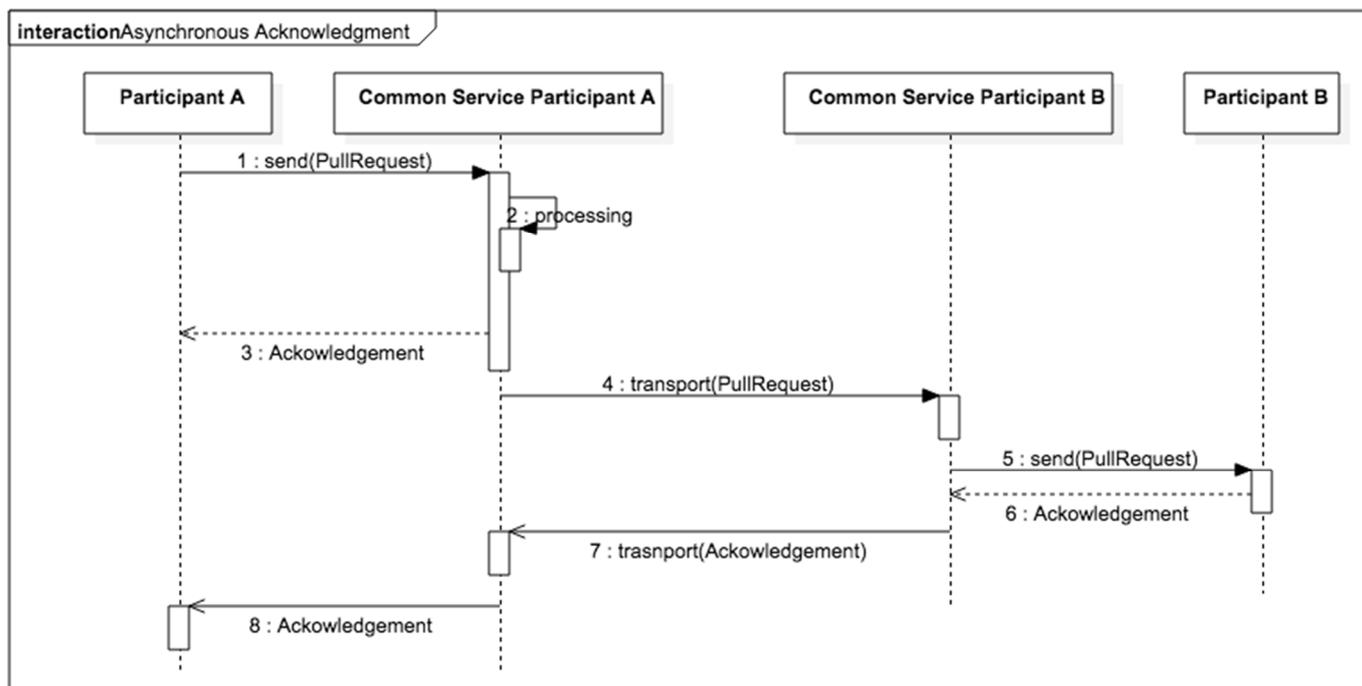

Figure 50: Common Services asynchronous acknowledgment

8.1.10   Message Signature

XML Signature (also called XMLDSig, XML-DSig, XML-Sig) defines an XML syntax for digital signatures and is defined in the W3C recommendation XML Signature Syntax and Processing [3].

In the CISE network, the XML Signature is one of the actions to ensure the secure transfer of information between participants. By signing the message, sender and recipients of a message ensure that along the transfer process it has not been changed or tempered in any way.
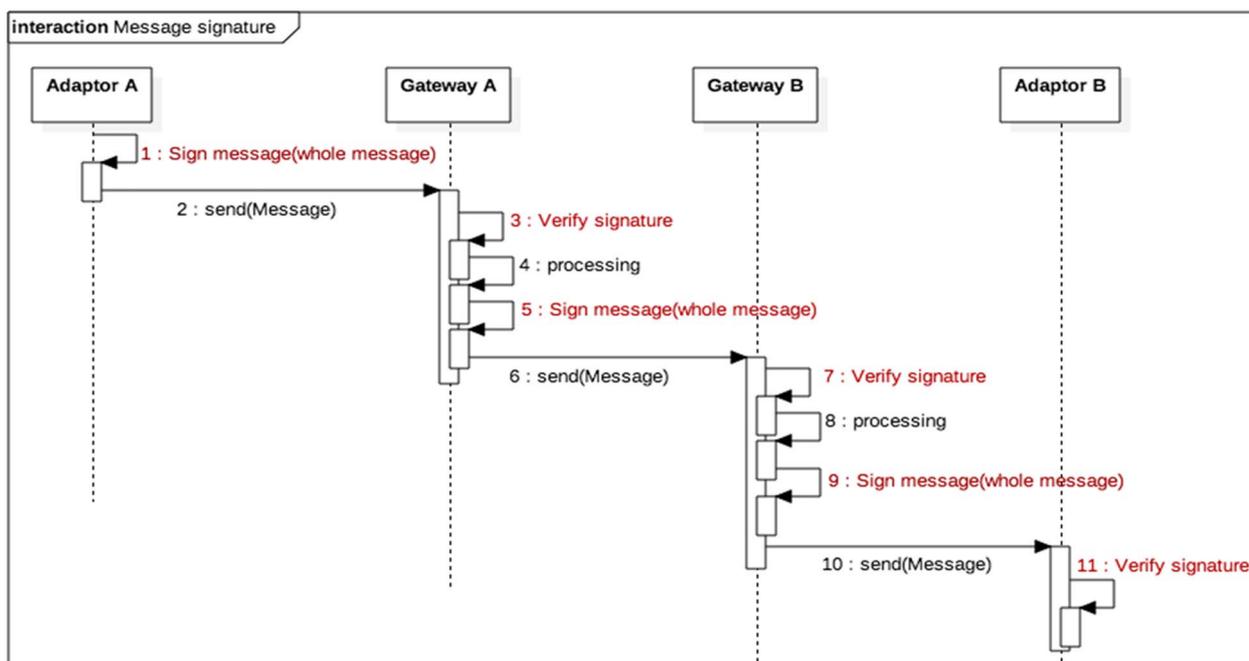
Figure 51: Message signature/verification

The previous diagram describes the steps taken regarding the message signature and verification along the message exchange process from one origin Adaptor to the destination.

To ensure the correct signature and validation of CISE Messages, all participants shall comply with the following:

- XML Signature Syntax and Processing element namespace [4].

- Canonicalization Method: INCLUSIVE [5]

- Transformation: ENVELOPED [3] (https://www.w3.org/TR/xmldsig-core1/#sec-EnvelopedSignature)

- Signature method: RSA_SHA1 [3] (https://www.w3.org/TR/xmldsig-core1/#sec-PKCS1)

- Digest method: SHA1 [3] (https://www.w3.org/TR/xmldsig-core1/#sec-SHA-1)

- Signature key: X.509 [6] certificate

NOTE: Due to variations in the message handling between different Adapter implementations (and more precisely because of the Payload element which is a "xs:any" type), it is possible that sometimes additional namespaces might be added that could not have been present in the message signature moment, resulting in failure to verify if the namespace is not also there. Because of this, it is advisable, before signature and verification, to remove any namespace that could exist in the Payload xml element.

The following excerpt is an example of a signed PullRequest message.

```
<?xml      version="1.0"      encoding="UTF-8"      standalone="no"?><ns4:PullRequest
xmlns:ns4="http://www.cise.eu/servicemodel/v1/message/"
xmlns:ns2="http://www.cise.eu/servicemodel/v1/authority/"
xmlns:ns3="http://www.cise.eu/servicemodel/v1/service/"><CorrelationID>549065e1-
fbbc-43e2-9f6a-2b7e4d56b869</CorrelationID><CreationDateTime>2017-11-
06T15:33:21.660Z</CreationDateTime><MessageID>549065e1-fbbc-43e2-9f6a-
2b7e4d56b869</MessageID><RequiresAck>true</RequiresAck><Sender><ServiceID>pt.for
necedor.ais.gtw1.aisstreams</ServiceID><ServiceOperation>Push</ServiceOperation>
<ServiceType>VesselService</ServiceType></Sender><Recipient><ServiceID>pt.fusion
.serv.service.1</ServiceID></Recipient><Payload
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns4:XmlEntityPayload"><InformationSecurityLevel>EUSecret</InformationS
ecurityLevel><InformationSensitivity>Amber</InformationSensitivity><Purpose>VTM<
/Purpose><Vessel><Name>BLUE
OCEAN</Name><MMSI>111111</MMSI></Vessel></Payload><PullType>Request</PullType><R
esponseTimeOut>-
2147483648</ResponseTimeOut><PayloadSelector><Selectors><Selector>//Payload/Vess
el[1]/Name</Selector><Operator>EQUAL</Operator></Selectors></PayloadSelector><Si
gnature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/><SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><Reference
URI=""><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>h1yA3qzDSlNVEWj
BnTNqsPrsRTk=</DigestValue></Reference></SignedInfo><SignatureValue>kCT2fx8GDu3J
LPFiIW+frkpNulj+XU4MMCUdHdNAF1xzeP5wbX2RvRnlf4OvkK4nNBffhuzJgjI5
iSlrU7ZdtyPzjiReiQB4bOR2VunceeRUI77Dkhyb0m3kFx7sF1tDEVji+a7VTYOaiURQFEPSHlV3
6u356DJ3BAZHgttV/iN412ZOy5u9IiJJsUw0D8w3kbiV3E7KftiC7qHllDBZDAsacPVUm/iUvvzl
snLHXtKmhyc/yOqvwzTEmtHXWczeaY5SW70QyZjJLmEQP7diXCpW8QrqQCThj06tPue5kLOPtepT
PuqeqCyQ+4Lt9OZqwjqw3dQfa7ze3Z+LuIwLhA==</SignatureValue><KeyInfo><X509Data><X50
9SubjectName>CN=prxy01-gw02.gw02.eucise.it,      OU=Hosts,      O=it,      DC=eucise,
C=it</X509SubjectName><X509Certificate>MIID6jCCAtKgAwIBAgIBHzANBgkqhkiG9w0BAQUFA
DBjMQswCQYDVQQGEwJpdDEWMBQGCgmSJomT
8ixkARkWBmV1Y2lzZTEdMBsGA1UECwwUZXVjaXNlLml0IHNpZ25pbmcgQ0ExHTAbBgNVBAMMFGV1
Y2lzZS5pdCBzaWduaW5nIENBMB4XDTE3MDcxMDE0Dk1NVoXDTE5MDcxMDE0Dk1NVowZzELMAkG
A1UEBhMCaXQxFjAUBgoJkiaJk/IsZAEZFgZldWNpc2UxCzAJBgNVBAoMAml0MQ4wDAYDVQQLDAVI
b3N0czEjMCEGA1UEAwwacHJ4eTAxLWd3MDIuZ3cwMi5ldWNpc2UuaXQwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCuDsFrrqsOkX3g0lUwYAkooF6cdYt6+a2p2owb4ycJ4yHX+6ZAf795
Ggra/J/kWFafN2pcbsrqfiL2IEH9oyHi9fnwlAcQBF+MiijBleQwUWptUjSRu/oPMFK1Ks3afVMj
```

1L9Y0lF2ZEYuvano/YkAgr3BNMCjm798Oas4GA6vt7EEtVdtOYn4yrycBp+P38R4Y81ER8XUbYez
+9y+EJEHG93FZQKuuiDZZwdS1/pk24JoR4fIA4Vkd78p5QYZVBCWYL+IUyywNX+p4ysp4O/rxUBG
YtujyPXA21ggRCctAEdx9JUjLRj6K1IjMevJhbr+gaRnj9ggDfea0qRf8fVzAgMBAAGjgaQwgaEw
DgYDVR0PAQH/BAQDAgWgMAkGA1UdEwQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MB0GA1UdDgQWBBQY3PPYiMTltcl3TDk/KUTjTMMHBTAfBgNVHSMEGDAWgBTw6Mux0dw5vMiSjPqk
IreUEtmDyzAlBgNVHREEHjAcghpwcnh5MDEtZ3cwMi5ndzAyLmV1Y2lzZS5pdDANBgkqhkiG9w0B
AQUFAAOCAQEAPEjeQryt/N2rBejI7xEF9TItsl4hTHAz/IuR1QiTL8dOhjXHmwo1ctb2LqrDzPiS
onke03lddfmPJ6UosOx9gX5tuyp6ZmDozEfgzjYpKbM5mqAaikOMIZ95XXdic/lxIZNbXNVhCRcv
h+bi+Ynoi/HUFNSvuqJ4ikW2xpCbnzkUGDBFaYelv1GoesKk02S8tALTJSMTCI2naX+c1wWIoJsy
YbkUYsW50/KaYPpmSqCY8LbBmMJFoBj+oN4Ec/k6zCI6DGiGLbrsGX9r3re0TFkAii4eQQbeEZIQ
uQha/ltOMn1Sy8zKldvHzx5al65V2lLmojm34Al2ku1WHlSAVQ==</X509Certificate></X509Data
></KeyInfo></Signature></ns4:PullRequest>

Annex A (informative):
Bibliography

- CISE Architecture Visions Document V3.0, 06/11/2013.

- JRC Technical Report: The Entity Service Model for CISE V1.5, 28/02/2017.

History

Document history		
V1.0.0	September 2021	Publication