

ETSI GS CDM 004 V1.1.1 (2024-07)



Common information sharing environment service and Data Model (CDM); Service Model; Release 1

Disclaimer

The present document has been produced and approved by the european Common information sharing environment service and Data Model (CDM) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

Reference

RGS/CDM-0010

Keywords

data models, maritime, protocol

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:

<https://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/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

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.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	10
3.3 Abbreviations	10
4 Overview	10
5 The CISE information services	11
5.1 Introduction	11
5.2 Sequence Diagrams	12
5.2.1 General.....	12
5.2.2 Pull (Request/Response).....	12
5.2.3 Push (known/unknown)	16
5.2.4 Publish/Subscribe	18
5.2.5 Discover.....	21
5.2.6 Feedback.....	22
6 The CISE Service Model.....	23
6.1 Global definitions	23
6.2 The Service Class	25
6.2.1 Service Class General Requirements	25
6.2.2 Enumeration.....	29
6.3 The Message Class	32
6.3.1 Message Class General Requirements	32
6.3.2 Enumeration.....	34
6.3.3 Message Extensions	36
6.3.3.1 Acknowledgment	36
6.3.3.2 Feedback	37
6.3.3.3 PullRequest	37
6.3.3.4 PullResponse.....	39
6.3.3.5 Push.....	39
6.4 The Participant Class.....	40
6.4.1 Participant Class General Requirements.....	40
6.4.2 Enumeration.....	42
6.5 Message Signature.....	42
6.5.1 General Requirements.....	42
Annex A (informative): Change History	44
History	45

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

On October 2009 the European Commission adopted the communication COM/2009/538 [i.3], promoting to integrate maritime surveillance activities of all public maritime sectors across Europe.

This Communication introduced the first general guiding principles of the Common Information Sharing Environment (CISE) and initiated the CISE development process (Figure 1).

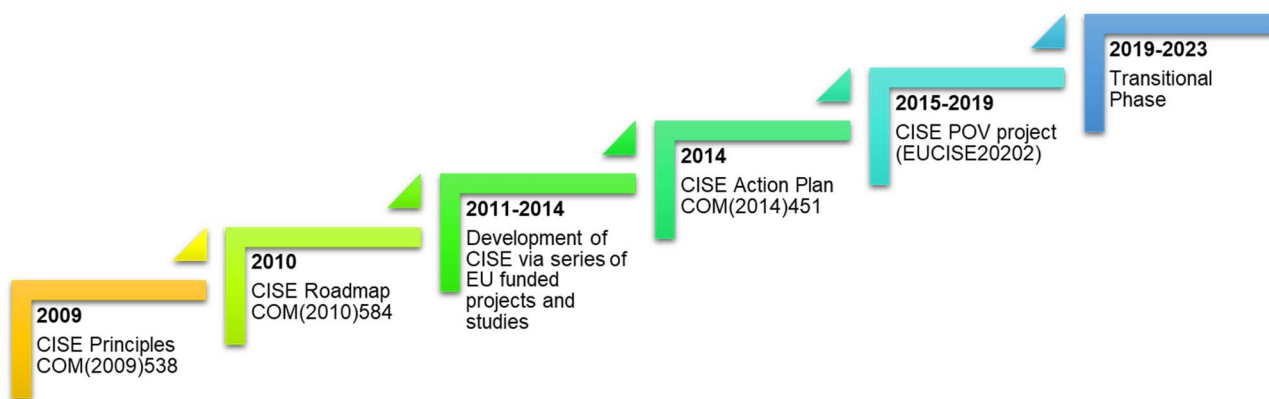


Figure 1: CISE development process

The Communication stated among other things, that the aim of the integrated maritime surveillance is to generate a situational awareness of activities at sea, impacting on the denominated seven maritime sectors: Maritime Safety and Security, Border Control, Maritime Pollution and Marine Environment Protection, Fisheries Control, Customs, General Law Enforcement and Defence, as well as the economic interests of the EU, so as to facilitate sound decision making.

Hybrid and complementary cross-sectoral and cross-border information exchange requires a common "data language" within the common network architecture as well as a common set of IT- services to handle the data transfer.

The technical standardization proposal for CISE implementation was therefore initiated by EUCISE 2020 project and directed towards a standardization process within the framework of a professional European standardization environment in order to elaborate universal and sustainable technical specifications for the implementation and development of CISE, as well as offering a technical solution for other, similar information exchange regimes.

The requirements in the present document respect the operational and technical requirements defined during the CISE development process (Figure 1) and the general principles of CISE as originally defined in [i.3] and [i.4] and later elaborated in the most recent version of the CISE Architecture [i.5] and [i.6] as follows:

- CISE connects public authorities in the EU and EEA responsible for maritime surveillance: civil and military, regional/sectorial organizations and EU agencies.
- CISE connects existing maritime surveillance ICT systems. However, CISE is not a new surveillance system, nor a new screen in the surveillance centres.
- CISE promotes a sector-neutral solution: all sectors and systems are important.
- CISE follows a decentralised approach: point-to-point exchange of information.
- Information exchange is voluntary, i.e. not enforced by legislation.

1 Scope

The present document provides terms and definitions for the Service Model of the European Common Information sharing environment service and Data Model (CDM), specifying the set of rules for sharing the elements of the CISE Data Model.

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>.

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.

- [1] [ETSI GS CDM 005](#): "Common information sharing environment service and Data Model (CDM); Data Model; Release 1".
- [2] [ISO 3166-1](#): "Codes for the representation of names of countries and their subdivisions, Part 1: Country codes".
- [3] [Recommendation ITU-T X.509](#): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- [4] [W3C® Recommendation 15 March 2001](#): "Canonical XMLVersion 1.0".
- [5] [W3C® Recommendation 12 February 2002](#): "XML-Signature Syntax and Processing".
- [6] [W3C® Recommendation 11 April 2013](#): "XML Signature Syntax and Processing Version 1.1".

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 002: "Common information sharing environment service and Data Model (CDM); System Requirements definition; Release 1".
- [i.2] ETSI GS CDM 003: "Common information sharing environment service and Data Model (CDM); CDM Architecture; Release 1".

- [i.3] [Communication from the Commission COM/2009/538 final](#) to the Council the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain.
- [i.4] [Communication from the Commission COM/2010/584 final](#) to the Council and the European Parliament on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain.
- [i.5] [CISE Architecture Visions Document, Version 3.0, 06/11/2013](#).
- [i.6] [CISE Architecture, Version 2.0, 04/03/2022](#).
- [i.7] [Service Model Guidelines - Building a CISE Adaptor](#).

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 (CA): 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: test project on cooperation in execution of various maritime functionalities at sub-regional or sea-basin level in the field of integrated maritime surveillance

NOTE: Project financed by the European Commission in 2013 defining the CISE use cases and the first version of the CISE data and service model.

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

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

EUCISE2020: European test bed for the maritime Common Information Sharing Environment in the 2020 perspective

NOTE 1: This FP7 project developed the existing CISE Network and software (2014-2019).

NOTE 2: More information on the project can be found at <https://cordis.europa.eu/project/id/608385>.

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 (LS): software designed to perform specific tasks and that exposes certain functionalities through interfaces

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

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: who manages the node's subsystems and the creation of new Adaptors

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

participant: Legacy System connected to the CISE network for exchanging data

provider: participant providing services over CISE network

public authority: any government or other public administration, including public advisory bodies, at national, regional or local level, performing public administrative functions under national law, including specific duties, activities or services

NOTE: 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)

Representational State Transfer (REST): architectural style for providing standards between computer systems on the web It leverages the capabilities of Hypertext Transfer Protocol (HTTP) and Uniform Resource Identifiers (URIs) to retrieve or modify the state of a resource

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

Transport Layer Security (TLS): cryptographic protocol designed to provide communications security over a computer network

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:

ACK	ACKnowledgment
CA	Certification Authority
CDM	CISE Data Model
CISE	Common Information Sharing Environment
EEA	European Economic Area
EU	European Union
FBK	Feedback
FP7	7 th Framework Programme
Gen	General
GS	Group Specification
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology
ID	Identifier
ISO	International Organization for Standardization
IT	Information Technology
LS	Legacy System
MSG	Message
PAR	Participant
PKI	Public Key Infrastructure
PRQ	Pull Request
PRS	Pull Response
PUS	Push
REST	Representational State Transfer
SAR	Search And Rescue
SER	Service
SIG	Signature
SOA	Service Oriented Architecture
TLS	Transport Layer Security
UML	Unified Markup Language
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VTM	Vessel Traffic Management
XML	eXtensible Markup Language
XPATH	W3C [®] XML Path language

4 Overview

The present document describes the CISE Service Model to support the requirements defined in ETSI GS CDM 002 [i.1] and ETSI GS CDM 003 [i.2] for the implementation the European Common Information sharing environment.

Clause 5 informs on how the CISE Service Model can be used to exchange messages between CISE participants, describing the CISE information flow and how the communication patterns are implemented.

Clause 6 provides the specification of the CISE Service Model.

The service types and the related information that can be exchanged over the CISE Services are described in ETSI GS CDM 005 [1].

5 The CISE information services

5.1 Introduction

The CISE Network is a complex open computer network interfacing several EU countries, specifically, in the maritime data context.

ETSI GS CDM 003 [i.2] defines a set of building blocks that are used in CISE to enable the information exchange between authorities of given Member States ("CISE Participants"):

- **CISE Node**, which manages the communication protocol among participants.
- **Adaptor**, which translates the CISE data and service model into the specific formats and communication protocols used by the Legacy System.
- **Legacy System**, which represents a new or an existing ICT system owned by a stakeholder that holds and/or requires information that could be exchanged through CISE.

CISE information services are provided by the adaptors/legacy systems and offered/published in the CISE Node.

When acting in CISE, a participant can play the role of provider, when it wants to send an information to a CISE participant, or the role of consumer, when it wants to receive an information from a CISE participant.

CISE Participants register their information services in the Service Registry of the CISE Node they belong to. This helps to understand which information is available in the network and what can be expected from the information services.

When acting as a service provider, a CISE participant defines an Access Right Matrix to set the access rules that authorize other participants to consume the information service of interest.

The exchange of information between CISE Participants is carried out on the basis of a communication protocol which provides the following patterns:

- **Pull**: the consumer knows the exact list of suppliers and asks for information; the information requested is made available only if and when possible (asynchronous pattern) after verifying that the consumer is authorized to receive the data.
- **Pull Unknown**: the consumer needs some information, but does not know who could provide it. The consumer asks for the information to all the possible providers. The information is made available only if and when possible (asynchronous pattern) by one or several providers, after verifying that the consumer is authorized to receive the data.
- **Push**: the provider knows a consumer possibly interested in some information and sends this information to the consumer (synchronous pattern).
- **Push Unknown**: the provider does not know who could need the information, but the provider sends it (synchronous pattern) to all the possible consumers of a certain profile.
- **Publish/Subscribe**: the consumer subscribes to a piece of information from the provider. When the piece of information is available in the provider, the provider sends it to all the consumers previously subscribed.

These 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.

5.2 Sequence Diagrams

5.2.1 General

The following clauses describe how a CISE Adaptor can communicate with a CISE Node to request or to provide CISE services.

The sequence diagrams that are relevant for the CISE information exchange are presented.

5.2.2 Pull (Request/Response)

The Pull communication pattern is used to send an information to a consumer that makes a request.

The communication flow is structured among two different and asynchronous phases: the Pull Request and the Pull Response.

Figure 5.2.2-1 shows the information flow of a pull request, which consists of the following steps:

- 1) The consumer CISE Adaptor prepares, signs and sends the pull request message to the CISE Node X it belongs to. The pull request message includes the provider details (i.e. CISE participant that receives the pull request) and the values of the request's attribute.
- 2) The CISE Node X sends the pull request message to the CISE Node Y (i.e. the CISE Node the provider CISE Adaptor belongs to).
- 3) The CISE Node X sends the acknowledgement to the consumer CISE Adaptor indicating that the pull request message has been sent to the CISE Node Y.
- 4) The CISE Node Y verifies that the consumer CISE Adaptor is authorized to receive the pull response.
- 5) The CISE Node Y sends the pull request message to the provider CISE Adaptor.
- 6) The CISE Node Y sends to the CISE Node X the acknowledgement indicating that the pull request message has been delivered.
- 7) If the consumer CISE Adaptor sets on the pull request message the field "requiresAck" to true, the CISE Node X sends to the consumer CISE Adaptor the acknowledgement indicating that the pull request message has been delivered to the provider CISE Adaptor.

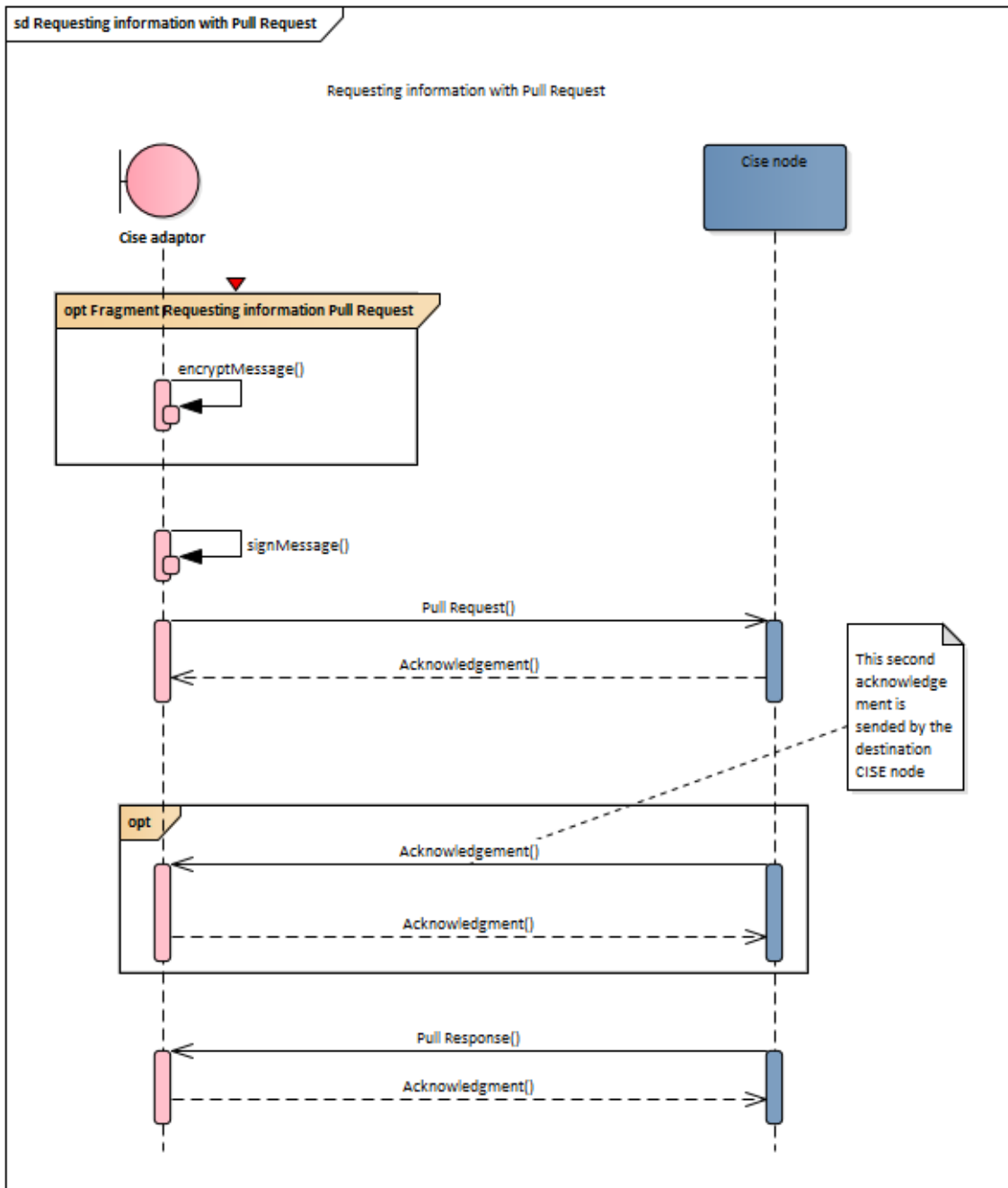


Figure 5.2.2-1: Flow of a Pull Request/Response
(Source: [i.7])

The Pull communication pattern also supports the case when a consumer needs some information but does not know who could provide it. This method is called Pull Request Unknown or Multicast.

In this case, the consumer asks for the information supplying a profile describing the service with the Discovery Profile instead of the Recipient.

Figure 5.2.2-2 shows the information flow of a pull request unknown, which consists of the following steps:

- 1) The consumer CISE Adaptor prepares, signs and sends the pull request message to the CISE Node X it belongs to. The pull request message includes the discovery profiles of the service it is interested in.
- 2) The CISE Node X using the discovery profile identifies the list of services and sends it to the consumer CISE adaptor by means of an acknowledgment message.

- 3) For each one of the identified services, the CISE Node X sends the pull request message to the CISE Node Y (i.e. the CISE Node the provider CISE Adaptor belongs to).
- 4) The CISE Node X sends the acknowledgement to the consumer CISE Adaptor indicating that the pull request message has been sent to the CISE Node Y.
- 5) The CISE Node Y verifies that the consumer CISE Adaptor is authorized to receive the pull response.
- 6) The CISE Node Y sends the pull request message to the provider CISE Adaptor.
- 7) The CISE Node Y sends to the CISE Node X the acknowledgement indicating that the pull request message has been delivered.
- 8) If the consumer CISE Adaptor sets on the pull request message the field "requiresAck" to true, the CISE Node X sends to the consumer CISE Adaptor the acknowledgement indicating that the pull request message has been delivered to the provider CISE Adaptor.

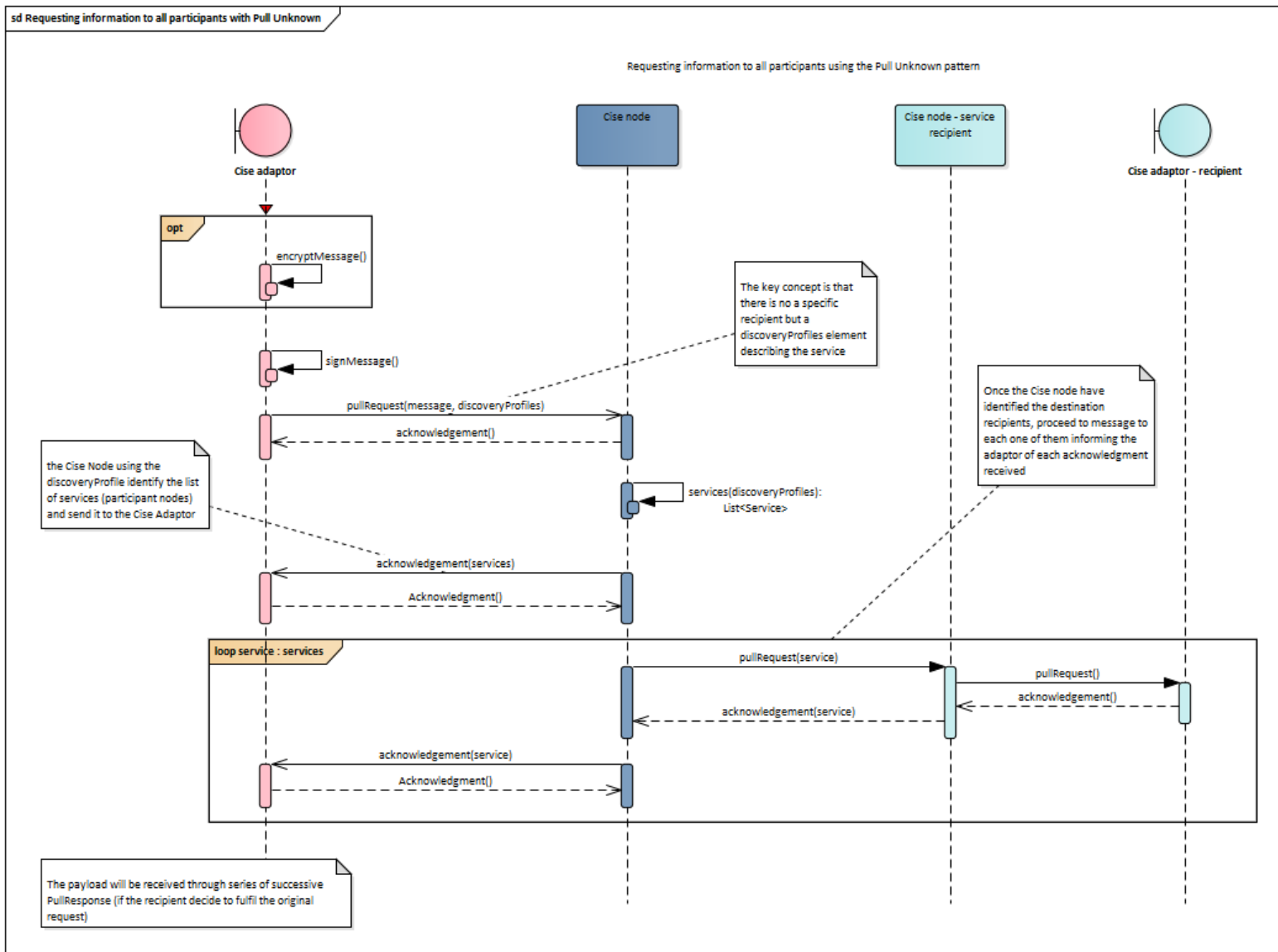


Figure 5.2.2-2: Flow of a PullRequest Unknown (Source: [i.7])

5.2.3 Push (known/unknown)

The Push to a known consumer pattern consists of the following steps:

- 1) The provider CISE Adaptor prepares, signs and sends the push message to the CISE Node X it belongs to. The push message includes the consumer details (i.e. CISE participant that receives the push message) and the attributes of the information to be sent.
- 2) The CISE Node X verifies that the consumer is authorized to receive the push message.
- 3) The CISE Node X sends the push message to the CISE Node Y (i.e. the CISE Node the consumer CISE Adaptor belongs to).
- 4) The CISE Node Y sends the push message to the consumer CISE Adaptor.
- 5) The CISE Node Y sends an acknowledgment to the CISE Node X.
- 6) If the provider CISE Adaptor sets on the pull request message the field "requiresAck" to true, the CISE Node X sends to the Provider Adaptor the acknowledgement indicating that the pull response message has been delivered to the consumer CISE Adaptor.

When the recipient (i.e. consumer CISE Adaptor) is unknown to the sender (i.e. provider CISE Adaptor), the CISE Node supports the method is called Push Unknown or Multicast. In this case, the pattern consists of the following steps:

- 1) The provider CISE Adaptor prepares, signs and sends the push message to the CISE Node X it belongs to. The push message does not include the consumer details (i.e. CISE participant that receives the push message), but includes the discovery profile of the service.
- 2) The CISE Node X sends an acknowledgment to the provider CISE Adaptor.
- 3) Thanks to the discovery profiles values contained in the push message provided by the provider CISE adaptor, the CISE Node X retrieve the list of recipients filtering them by the internal service registry.

For each CISE participant included in the list of authorized consumers, the following steps are then performed:

- 4) The CISE Node X sends the push message to the CISE Node Y (i.e. the CISE Node the consumer CISE Adaptor belongs to).
- 5) The CISE Node Y sends the push message to the consumer CISE Adaptor.
- 6) The CISE Node Y sends an acknowledgment to the CISE Node X.
- 7) If the provider CISE Adaptor sets on the pull request message the field "requiresAck" to true, the CISE Node X sends to the provider CISE Adaptor the acknowledgement indicating that the pull response message has been delivered to the consumer CISE Adaptor.

Figure 5.2.3-1 shows the information flow of a push to unknown pattern.

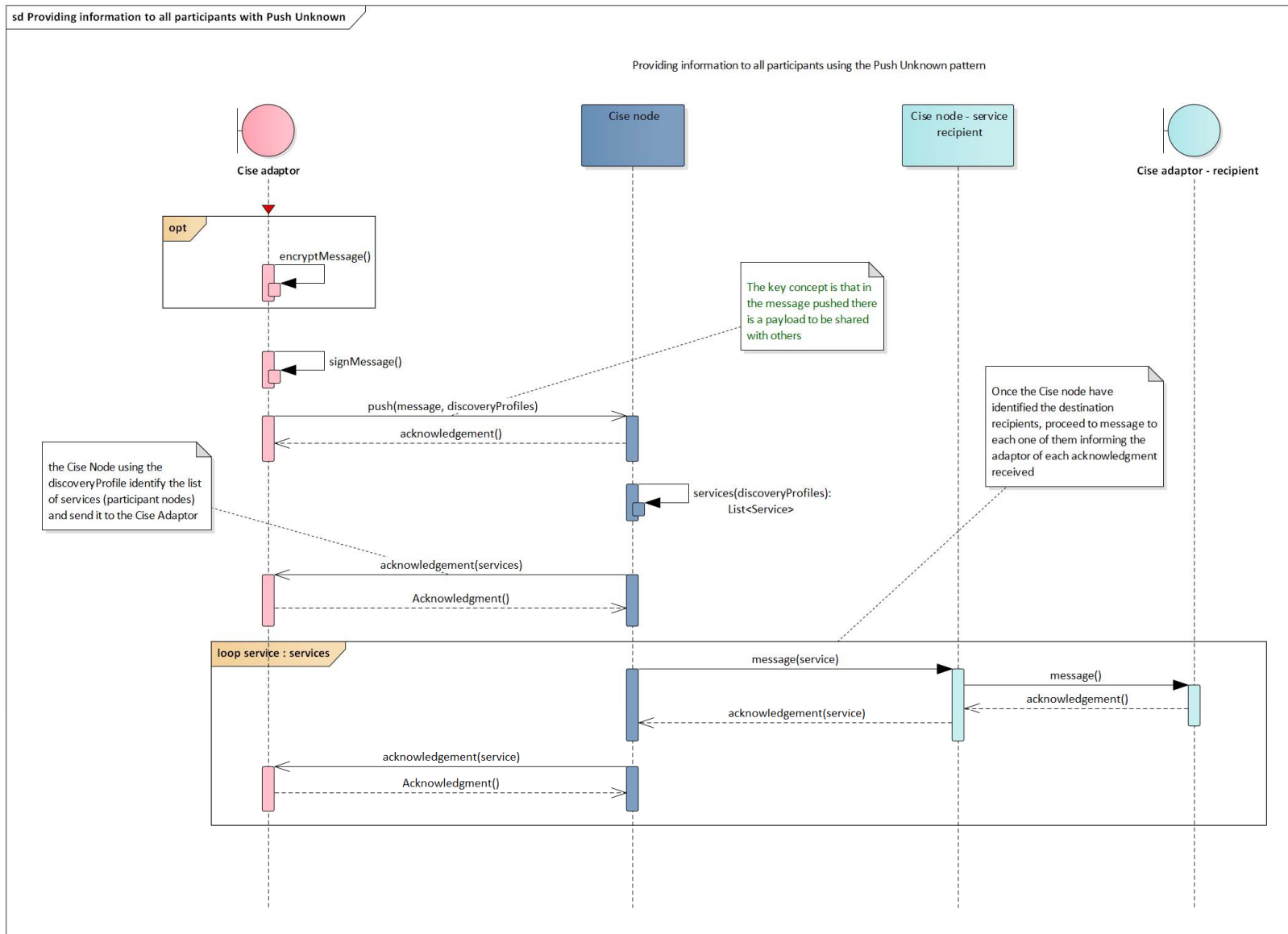


Figure 5.2.3-1: Flow of a Push to an unknown consumer (Source: [i.7])

5.2.4 Publish/Subscribe

The Publish/Subscribe Pattern is used for periodical exchange of messages between a provider and a list of subscribers.

The communication flow is structured among three different and asynchronous phases:

- The Subscription Request, which is handled by means of a Pull Request operation.
- The Publish Response, which is handled by a Push Response operation.
- The Unsubscription Request, which is handled by means of a Pull Request operation.

Figure 5.2.4-1 illustrates the subscribe request pattern that is based on the pull request method, already described in clause 5.2.2, when the pull type value is set to "Subscribe".

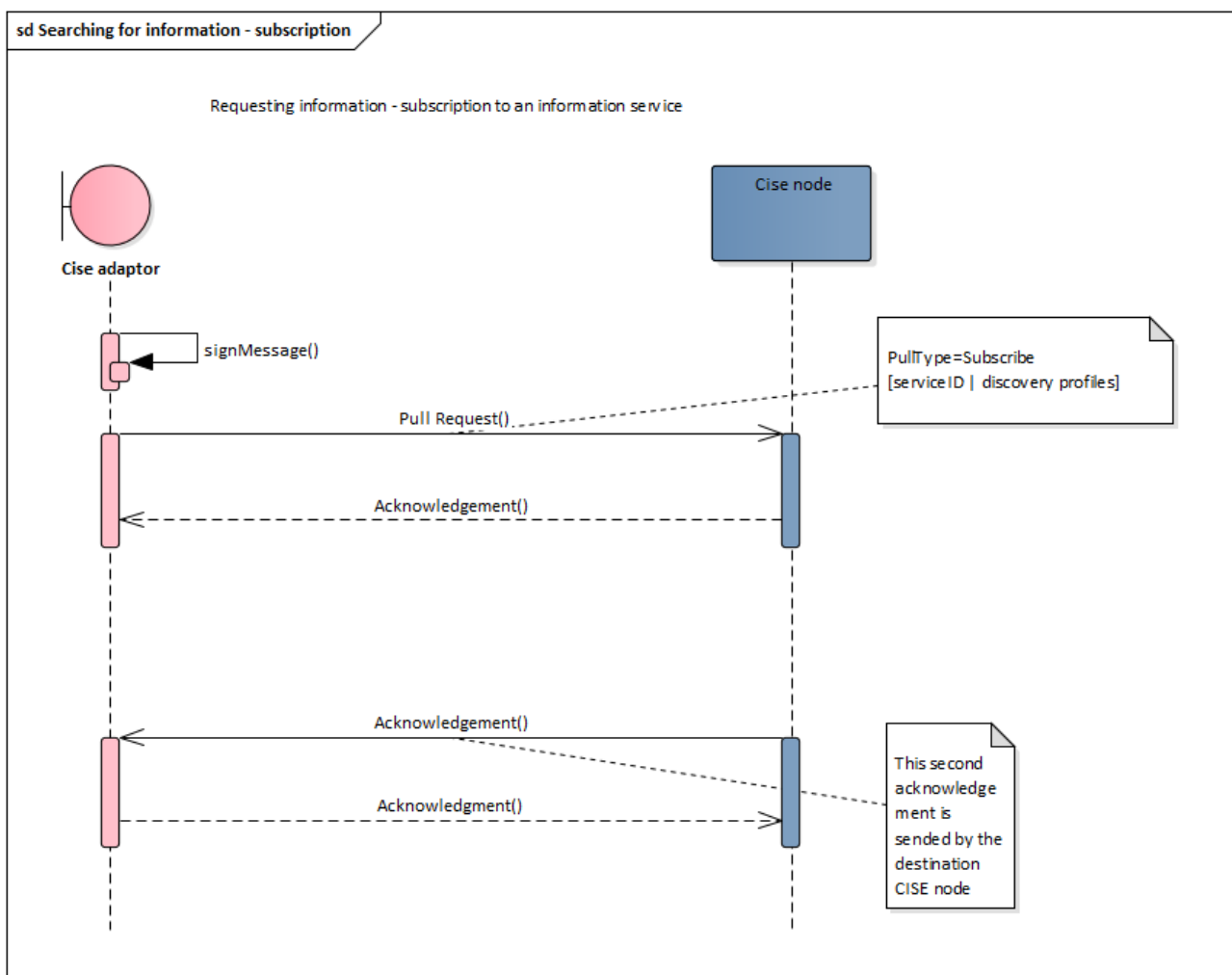


Figure 5.2.4-1: Flow of a Subscribe Request
(Source: [i.7])

The publish response pattern depends on the actor which handles the list of subscribers.

If the list of subscribers is handled by the provider CISE Adaptor, the publish response pattern is structured among the following steps:

- The provider CISE Adaptor prepares, signs and sends the pull request message to the CISE Node X it belongs to. The pull type value is set to "Get Subscribers".
- The CISE Node X sends an acknowledgment to the provider CISE Adaptor. The payload of the acknowledgement includes the list of CISE participant subscribers.

For each CISE participant included in the list of subscribers, the following steps are then performed:

- 3) The provider CISE Adaptor prepares, signs and sends the push message to the CISE Node X.
- 4) The CISE Node X verifies that the consumer is authorized to receive the push message.
- 5) The CISE Node X sends the push message to the CISE Node Y.
- 6) The CISE Node Y sends the push message to the consumer CISE Adaptor.
- 7) The CISE Node Y sends an acknowledgment to the CISE Node X.
- 8) If the provider CISE Adaptor sets on the pull request message the field "requiresAck" to true, the CISE Node X sends to the provider CISE Adaptor the acknowledgement indicating that the pull response message has been delivered to the consumer CISE Adaptor.

If the list of subscribers is handled by the CISE Node X, the publish response pattern is structured among the following steps:

- 1) The provider CISE Adaptor prepares, signs and sends the push message to the CISE Node X it belongs to. The service operation value is set to "Subscribe".
- 2) The CISE Node X sends an acknowledgment to the provider CISE Adaptor.
- 3) The CISE Node X retrieve the list of subscribers by the internal service registry.

For each CISE participant included in the list of subscribers, the following steps are then performed:

- 4) The CISE Node X sends the push message to the CISE Node Y.
- 5) The CISE Node X sends the push message to the consumer CISE Adaptor.
- 6) The CISE Node Y sends an acknowledgment to the CISE Node X.
- 7) If the provider CISE Adaptor sets on the pull request message the field "requiresAck" to true, the CISE Node X sends to the provider CISE Adaptor the acknowledgement indicating that the pull response message has been delivered to the consumer CISE Adaptor.

Figure 5.2.4-2 shows a Publish Response scenario where the list of subscribers is handled by the "provider" CISE Node.

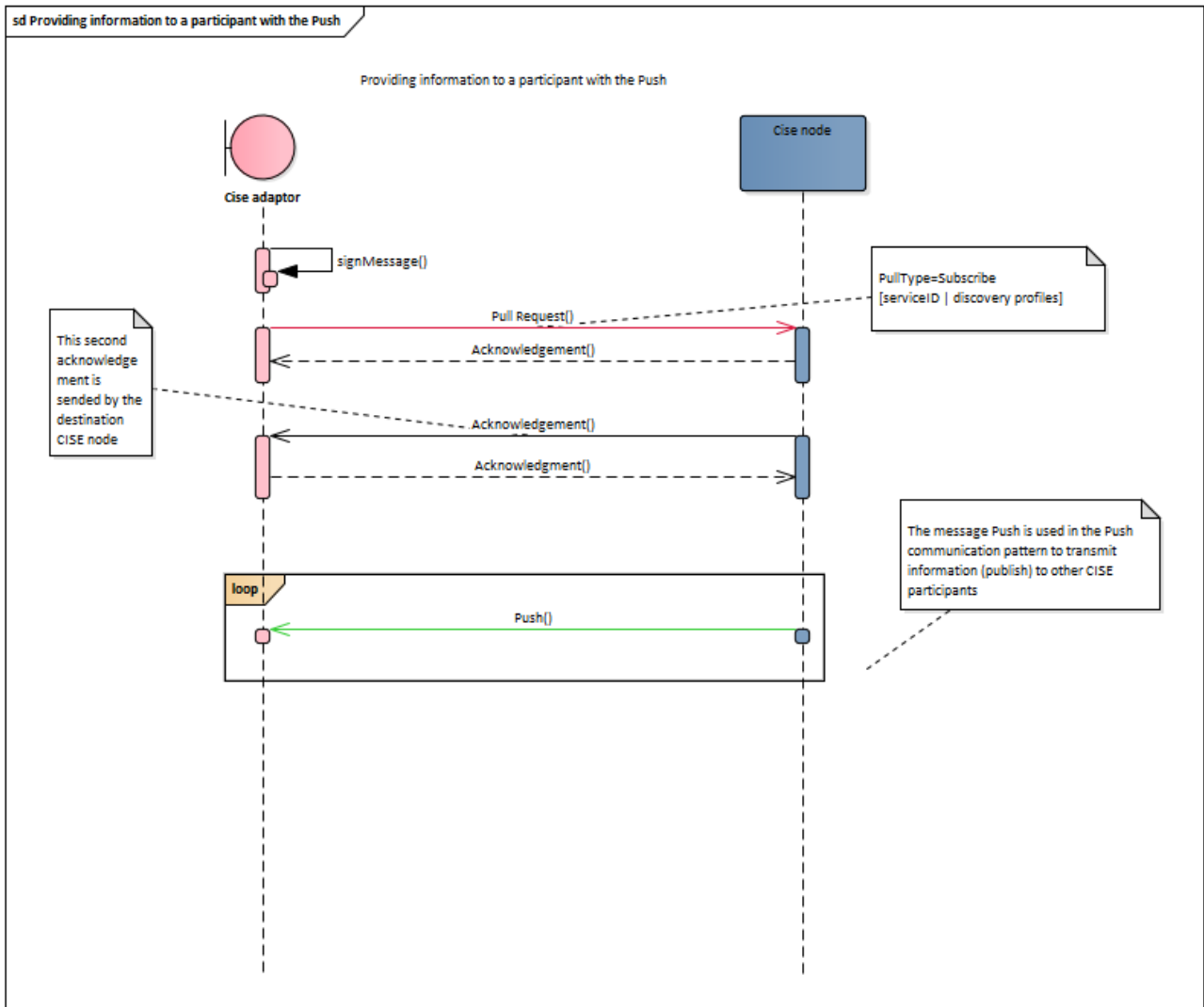


Figure 5.2.4-2: Flow of a Publish Response with subscribers list handled by the CISE Node (Source: [i.7])

Figure 5.2.4-3 illustrated the unsubscribe request pattern that is based on the pull request method, already described in clause 5.2.2, when the pull type value is set to "Unsubscribe".

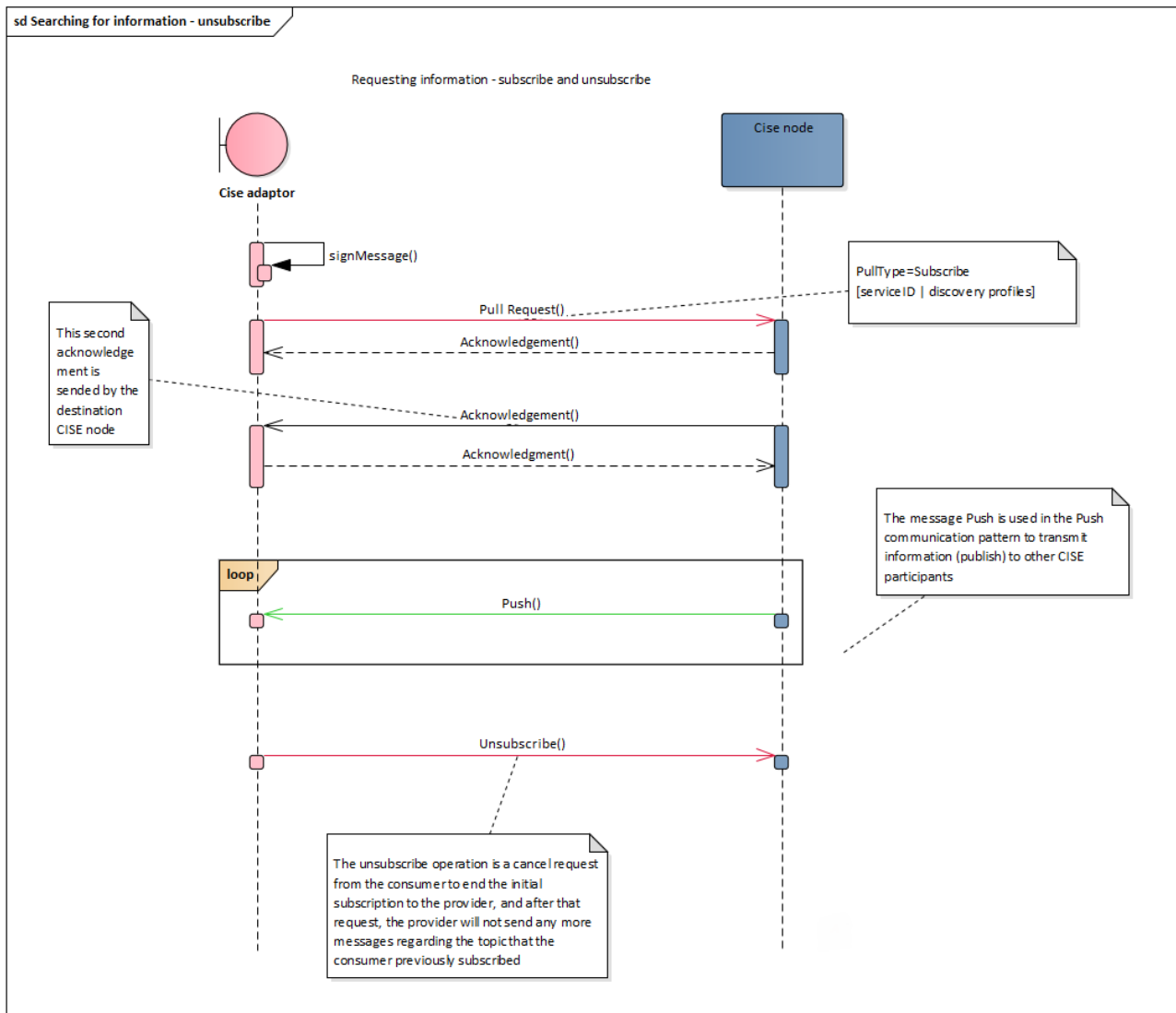


Figure 5.2.4-3: Flow of the Unsubscribe Request
(Source: [i.7])

5.2.5 Discover

The discover communication pattern is used by a CISE Participant to request a list of available CISE services. The discover pattern is a synchronous flow between a CISE Adaptor and a CISE Node and consists of the following steps:

- 1) The CISE Adaptor prepares, signs and sends the pull request message to the CISE Node it belongs to. The pull request message includes the pull type value set to "Discover".
- 2) The CISE Node sends the acknowledgement to the Adaptor, including in the payload the list of the services available on the CISE network which comply with the description provided in the DiscoveryProfile field set by the CISE Adaptor.

Figure 5.2.5-1 illustrates the Discover pattern.

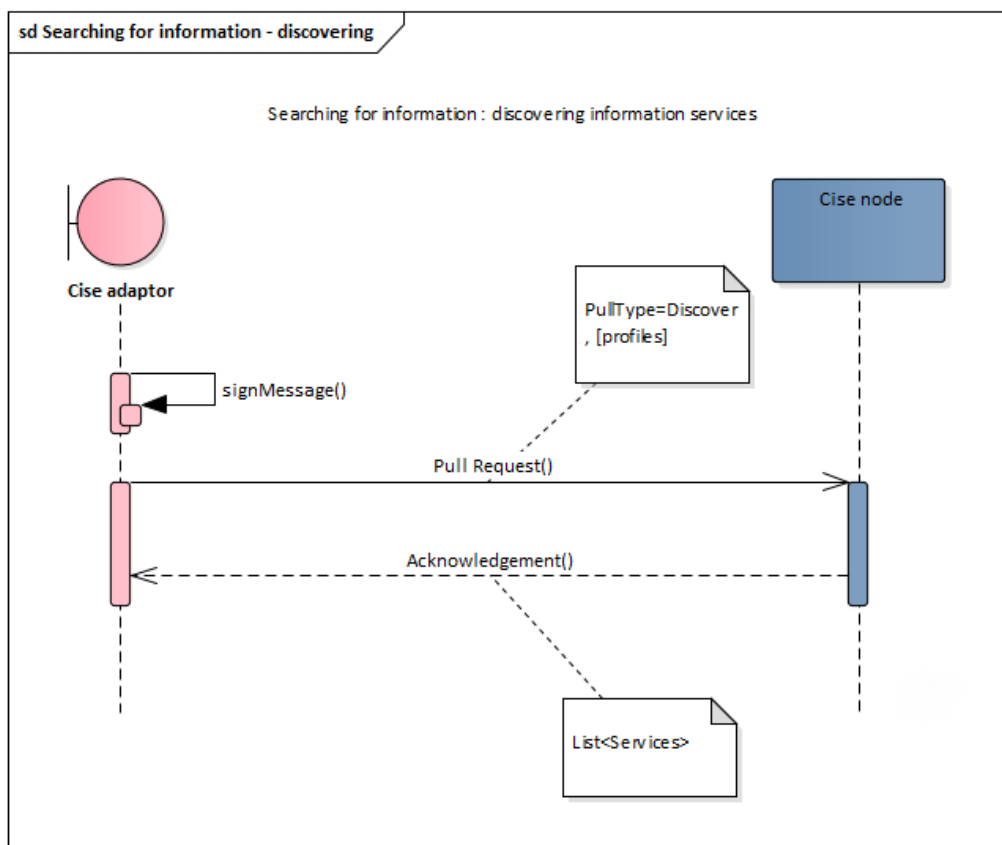


Figure 5.2.5-1: Flow of the Discover pattern
(Source: [i.7])

5.2.6 Feedback

The Feedback communication pattern is used by a CISE Adaptor to notify an add additional information related to a message already delivered to a CISE recipient or already received by a CISE participant.

The feedback pattern consists of the following steps:

- 1) The Provider Adaptor prepares, signs and sends the feedback message to the "provider" CISE Node it belongs to. The feedback message includes the correlation ID of the message the feedback refers to.
- 2) The "provider" CISE Node sends the acknowledgment to the Provider Adaptor.
- 3) The "provider" CISE Node sends the acknowledgment to the "consumer" CISE Node.
- 4) The "consumer" CISE Node sends the feedback message to the Consumer Adaptor.
- 5) The "consumer" CISE Node sends the acknowledgment to the "provider" CISE Node that the feedback message has been delivered to the Consumer Adaptor.
- 6) If the Provider Adaptor sets on the pull request message the field "requiresAck" to true, the "provider" CISE Node sends to the Provider Adaptor the acknowledgement indicating that the pull response message has been delivered to the Consumer Adaptor.

6 The CISE Service Model

6.1 Global definitions

[Ser-GEN-001] A CISE service shall be described by the following classes:

- Service.
- Message.
- Participant.

[Ser-GEN-002] The service class shall provide the **description of the attributes** of a CISE service.

[Ser-GEN-003] The message class shall provide the **description of the contents** of a CISE service.

[Ser-GEN-004] The participant class shall provide the **description of the actors** involved in the exchange of a CISE service.

Figure 6.1-1 illustrates the CISE Service Model.

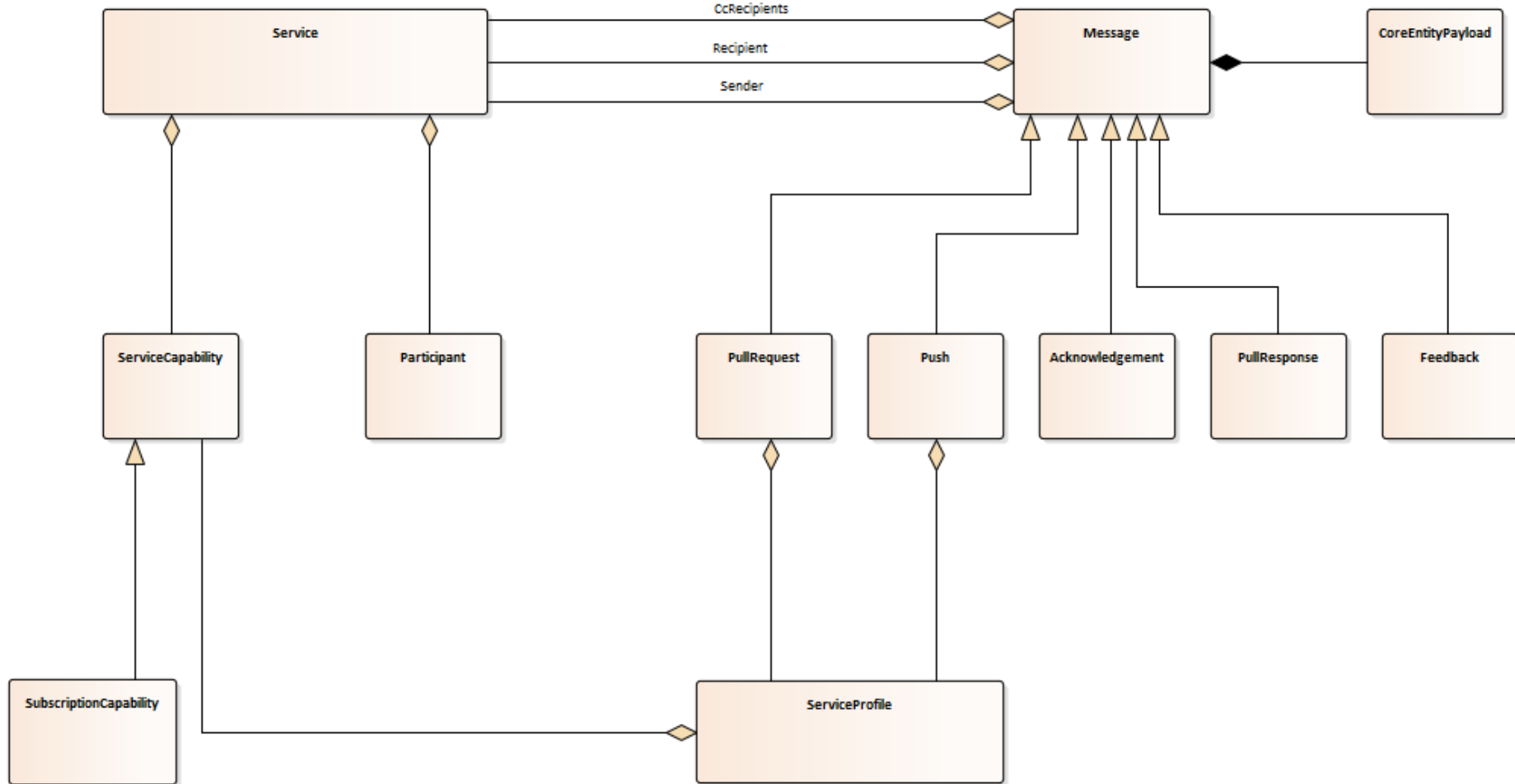


Figure 6.1-1: The CISE Service Model
(Source: [i.7])

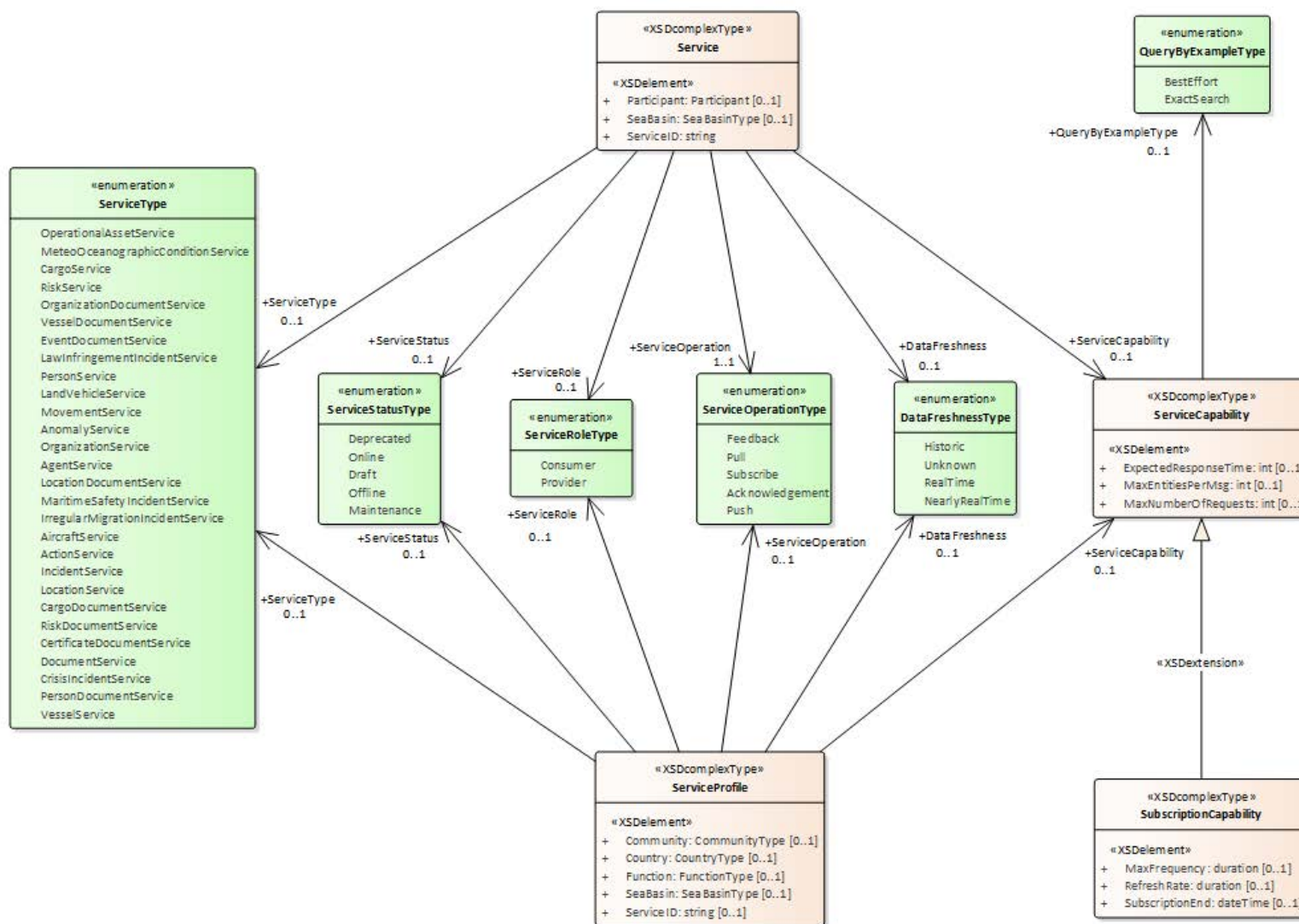
6.2 The Service Class

6.2.1 Service Class General Requirements

[Ser-SER-001] A CISE service shall be described by means of:

- **DataFreshness:** This field specifies what type of data is provided by the Service. This is to distinguish real time data from historical data.
- **Participant:** Participant to which the service belongs.
- **SeaBasin:** The sea basin covered by the service.
- **ServiceCapability:** The Capabilities provided by the service.
- **ServiceID:** This is the unique ID of the service.
- **ServiceOperation:** The type of communication pattern supported by the Service (e.g. Pull/Push/Subscribe/Feedback/Ack).
- **ServiceRole:** Role of the service in the message exchange process.
- **ServiceStatus:** The status of the Service.
- **ServiceType:** The type of entities exchanged based on the CISE Data Model.

Figure 6.2.1-1 illustrates the Service class.



The CISE service model (extract)

Figure 6.2.1-1: The Service class model (Source: [i.7])

Table 6.2.1-1 illustrates the data structure supported by the Service class.

Table 6.2.1-1: Data Structures supported by the Service class

Field Name	Data Type
DataFreshness	DataFreshnessType
SeaBasin	SeaBasinType
ServiceID	String
ServiceOperation	ServiceOperationType
ServiceRole	ServiceRoleType
ServiceStatus	ServiceStatusType
ServiceType	ServiceType
Participant	ParticipantType
ServiceCapability	ServiceCapabilityType

[Ser-SER-002] The description of a CISE service shall be supported by a ServiceProfile structure.

[Ser-SER-003] The ServiceProfile shall define the following attributes:

- **Community:** One of the 7 user communities participating to CISE.
- **Country:** The Country of the provider of the service.
- **DataFreshness:** This field specify what type of data is provided by the service.
- **Function:** The mission covered by the provider of the service.
- **SeaBasin:** The sea basin of covered by the service.
- **ServiceCapability:** The Capabilities provided by the service.
- **ServiceID:** This is the unique ID of the service.
- **ServiceOperation:** The type of communication pattern supported by the service (e.g. Pull, Push, Subscribe, Feedback and Ack).
- **ServiceRole:** Role of the service in the message exchange process.
- **ServiceStatus:** The status of the service.
- **ServiceType:** The type of entities exchanged based on the CISE Data Model.
- **Subscription Capability:** Extension of the ServiceCapability data structure in case of a subscribe service.

Figure 6.2.1-2 illustrates the ServiceProfile class.

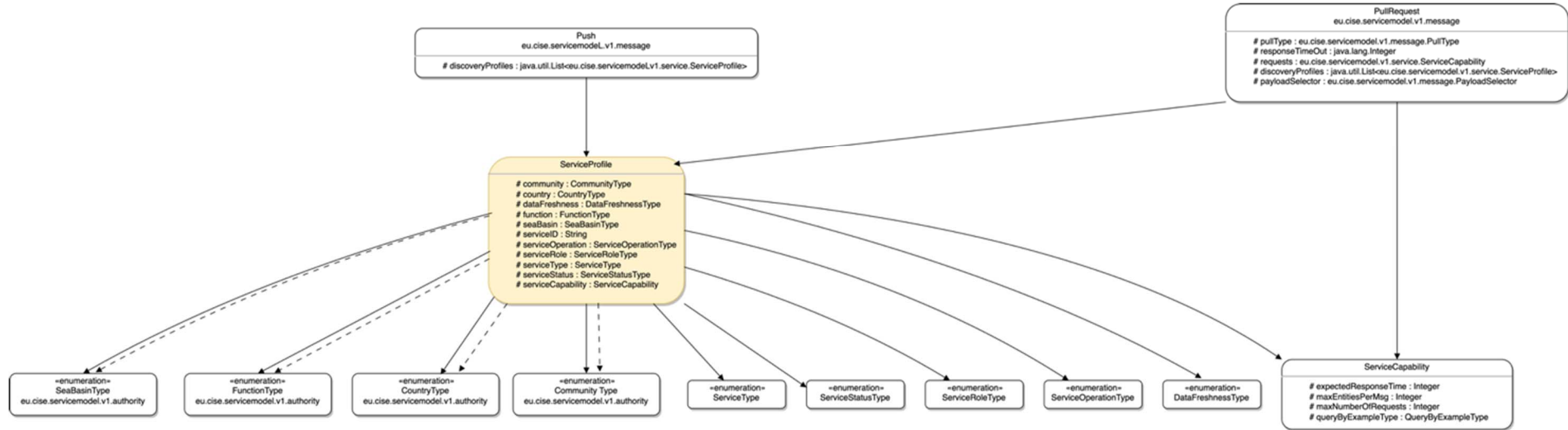


Figure 6.2.1-2: The ServiceProfile class model (Source: [i.7])

Table 6.2.1-2 illustrates the data structure supported by the ServiceProfile class.

Table 6.2.1-2: Data Structures supported by the ServiceProfile Class

Field Name	Data Type
Community	CommunityType
Country	CountryType
DataFreshness	DataFreshnessType
Function	FunctionType
SeaBasin	SeaBasinType
ServiceOperation	ServiceOperationType
ServiceRole	ServiceRoleType
ServiceID	String
ServiceType	ServiceType
ServiceStatus	ServiceStatusType
ServiceCapability	ServiceCapabilityType

The specification of the possible value of the Service Type field is included in the ETSI GS CDM 005 [1].

6.2.2 Enumeration

[Ser-SER-004] The CommunityType shall support the following values:

- GeneralLawEnforcement.
- Customs.
- MarineEnvironment.
- MaritimeSafetySecurity.
- DefenceMonitoring.
- FisheriesControl.
- BorderControl.
- Other.
- NonSpecified.

[Ser-SER-005] The CountryType shall be a 2 charactered country code compliant with the ISO-3166-1 [2] alpha-2 specifications.

[Ser-SER-006] The DataFreshness Type shall support the following values:

- Historic.
- RealTime.
- NearlyRealTime.
- Unknown.

[Ser-SER-007] The FunctionType shall support the following values:

- VTM.
- Safety.
- Security.
- SAR.

- Operation.
- FisheriesWarning.
- FisheriesMonitoring.
- FisheriesOperation.
- EnvironmentMonitoring.
- EnvironmentWarning.
- EnvironmentResponse.
- CustomsMonitoring.
- Customs Operation.
- BorderMonitoring.
- BorderOperation.
- LawEnforcementMonitoring.
- LawEnforcementOperation.
- DefenceMonitoring.
- CounterTerrorism.
- CSDPTask.
- NonSpecified.

[Ser-SER-008] The SeaBasinType shall support the following values:

- Atlantic.
- BalticSea.
- NorthSea.
- Mediterranean.
- BlackSea.
- OutermostRegions.
- ArcticOcean.
- NonSpecified.

[Ser-SER-009] The ServiceOperation Type shall support the following values:

- Pull.
- Push.
- Subscribe.
- Acknowledgement.
- Feedback.

[Ser-SER-010] The ServiceRole Type shall support the following values:

- Consumer.
- Provider.

[Ser-SER-011] The ServiceStatus Type shall support the following values:

- Draft.
- Online.
- Maintenance.
- Deprecated.
- Offline.

[Ser-SER-012] The ServiceCapability shall define the following attributes:

- **MaxEntitiesPerMsg:** Maximum number of entities returned in a pull response.
- **QueryByExampleType:** Type used for the query by example. This mechanism supports either exact answers or approximate answers.
- **ExpectedResponseTime:** Estimated average time to receive a response.
- **MaxNumberOfRequests:** Number of requests by hour allowed by the system providing.

Table 6.2.2-1 illustrates the data structure supported by the ServiceCapability

Table 6.2.2-1: Data structure of ServiceCapability

Field Name	Data Type	Note
MaxEntitiesPerMsg	Integer	
QueryByExampleType	QueryByExampleType	
ExpectedResponseTime	Integer	
MaxNumberOfRequests	Integer	Undefined = no limit

[Ser-SER-013] The SubscriptionCapability shall define the following attributes:

- **MaxFrequency:** Maximum frequency of update available.
- **RefreshRate:** Average time between two updates.
- **SubscriptionEnd:** Date and time when the subscription end.

Table 6.2.2-2 illustrates the data structure supported by the SubscriptionCapability

Table 6.2.2-2: Data structure of SubscriptionCapability

Field Name	Data Type	Note
MaxFrequency	Integer	Time in seconds.
RefreshRate	Integer	Time in seconds.
SubscriptionEnd	DateTime	

[Ser-SER-014] The QueryByExample Type shall support the following values:

- BestEffort.
- ExactSearch.

6.3 The Message Class

6.3.1 Message Class General Requirements

[Ser-MSG-001] A CISE message shall be described by means of:

- **Mandatory Attributes:**
 - **MessageID:** Unique identifier of the message.
 - **PriorityType:** Priority level.
 - **Sender:** Identification of the sender of the message.
- **Optional Attributes:**
 - **ContextID:** unique identifier that correlates messages that belong to messages exchange related to the same operational need.
 - **CorrelationID:** unique identifier that correlates messages that belong to the same thread of message exchange.
 - **CreationDateTime:** date and time of creation of the message.
 - **RequiresAck:** request for an asynchronous acknowledgment after the delivery of the message to the final recipient.
 - **Recipient:** identification of the recipient of the message.
 - **Payload:** the business payload of the message and the related metadata.
 - **ReliabilityProfile:** information about the retry strategy in case of error during the transmission of the message.
 - **CcRecipients:** participants the receive a notification when the message is delivered to the recipient.
- **Extended Attributes:**
 - **Acknowledgment:** specific attributes of the acknowledgment message.
 - **Feedback:** specific attributes of the feedback message.
 - **PullRequest:** specific attributes of the PullRequest message.
 - **PullResponse:** specific attributes of the PullResponse message.
 - **Push:** specific attributes of the Push message.

Figure 6.3.1-1 illustrates the Message Class.

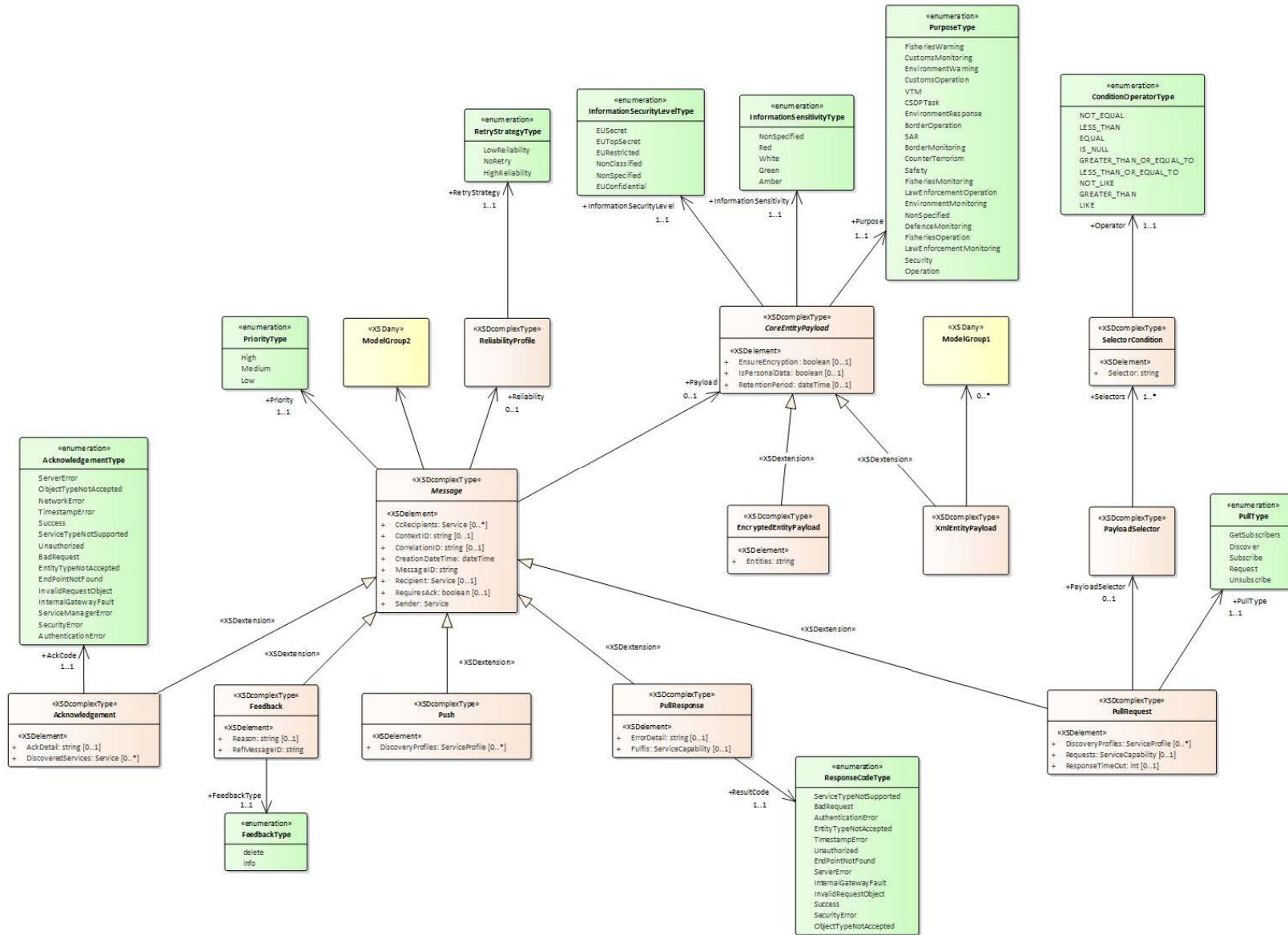


Figure 6.3.1-1: The Message Class UML conceptual Model (Source: [i.7])

Table 6.3.1-1 illustrates the data structure supported by the Message class.

Table 6.3.1-1: Data Structures supported by the Message class

Field Name	Data Type	Note
Acknowledgment	AcknowledgmentType	Message extension
CcRecipients	ParticipantType	
ContextID	String	UUID
CorrelationID	String	UUID
CreationDateTime	XMLGregorianCalendar	
Feedback	FeedbackType	Message extension
MessageID	String	UUID
Payload	CoreEntityPayloadType	
Priority	PriorityType	
PullRequest	PullRequestType	Message extension
PullResponse	PullResponseType	Message extension
Push	PushType	Message extension
Recipient	ServiceType	
ReliabilityProfile	RetryStrategyType	
RequiresAck	Boolean	
Sender	ParticipantType	

6.3.2 Enumeration

[Ser-MSG-002] The PriorityType shall support the following values:

- High.
- Low.
- Medium.

[Ser-MSG-003] The RetryStrategyType shall support the following values:

- HighReliability.
- LowReliability.
- NoRetry.

[Ser-MSG-004] The CoreEntityPayloadType shall define the following attributes:

- **InformationSecurityLevel:** Security level associated to the payload of the message.
- **InformationSensitivity:** Sensitivity level associated to the payload of the message.
- **IsPersonalData:** Boolean value to define if the payload of the message contains personal data.
- **Purpose:** The business need related to the exchange of the message.
- **RetentionPeriod:** in case of the payload contains personal data, this value defines the date and the time until when the payload can be handled.
- **EnsureEncryption:** Boolean value to indicate if the payload is encrypted.
- **Extended Attributes:**
 - **XMLEntityPayload:** if the payload is not encrypted, it contains the entities to be exchanged.
 - **EncryptedEntityPayload:** if the payload is to be encrypted, it contains the encrypted entities to be exchanged.

Table 6.3.2-1 illustrates the data structure supported by the CoreEntityPayload.

Table 6.3.2-1: Data structure of CoreEntityPayload

Field Name	Data Type	Note
InformationSecurityLevel	InformationSecurityLevelType	
InformationSensitivity	InformationSensitivityType	
IsPersonalData	Boolean	
Purpose	PurposeType	
RetentionPeriod	XMLGregorianCalendar	
EnsureEncryption	Boolean	
EncryptedEntityPayload	String	Encrypted data encoded in BASE64 format
XMLEntityPayload	XML	The content of this field will be checked with the data model XML Schema.

[Ser-MSG-005] The InformationSecurityLevelType shall support the following values:

- EUTopSecret.
- EUSecret.
- EUConfidential.
- EURestricted.
- NonClassified.
- NonSpecified.

[Ser-MSG-006] The InformationSensitiveType shall support the following values:

- Red.
- Amber.
- Green.
- White.
- NonSpecified.

[Ser-MSG-007] The PurposeType shall support the following values:

- VTM.
- Safety.
- Security.
- SAR.
- Operation.
- FisheriesWarning.
- FisheriesMonitoring.
- FisheriesOperation.
- EnvironmentMonitoring.
- EnvironmentWarning.
- EnvironmentResponse.
- CustomsMonitoring.

- CustomsOperation.
- BorderMonitoring.
- BorderOperation.
- LawEnforcementMonitoring.
- LawEnforcementOperation.
- DefenceMonitoring.
- CounterTerrorism.
- CSDPTask.
- NonSpecified.

[Ser-MSG-008] If the CoreEntityPayload has to be encrypted, the encryption method, cypher keys and algorithms shall be previously agreed and exchange between the participants sending and receiving the message.

6.3.3 Message Extensions

6.3.3.1 Acknowledgment

[Ser-ACK-001] The Acknowledgment message extension shall define the following attributes:

- **AckCode:** code representing the success in the transmission of the message or the type of fault occurred in the transmission.
- **Optional Attributes:**
 - **AckDetail:** additional textual description of the fault occurred.
 - **DiscoveredServices:** when used in Discovery or GetSubscribers communication pattern, it returns the list of discovered services or the list of subscribers.

Table 6.3.3.1-1 illustrates the data structure supported by the AcknowledgmentType.

Table 6.3.3.1-1: Data structure of AcknowledgmentType

Field Name	Data Type	Note
AckCode	AckCodeType	
AckDetail	String	Free text
DiscoveredServices	ServiceProfileType	Ref.to [ser-SER-003]

[Ser-ACK-002] The AckCodeType shall support the following values:

- Success.
- EndPointNotFound.
- SecurityError.
- InternalGatewayFault.
- InvalidRequestObject.
- Unauthorized.
- BadRequest.
- ServiceTypeNotSupported.

- EntityTypeNotAccepted.
- ObjectTypeNotAccepted.
- ServerError.
- TimestampError.
- AuthenticationError.
- NetworkError.
- ServiceManagerError.

6.3.3.2 Feedback

[Ser-FBK-001] The Feedback message extension shall define the following attributes:

- **FeedbackType:** The type of feedback to provide.
- **Reason:** A string that describes the reason for the feedback.
- **RefMessageId:** The unique ID of the message the feedback refers to.

Table 6.3.3.2-1 illustrates the data structure supported by the FeedbackType.

Table 6.3.3.2-1: Data structure of FeedbackType

Field Name	Data Type	Note
FeedbackType	FeedbackTypeType	
Reason	String	Free text
RefMessageID	String	UUID

[Ser-FBK-002] The FeedbackTypeType shall support the following values:

- Info.
- Delete.

6.3.3.3 PullRequest

[Ser-PRQ-001] The PullRequest message extension shall define the following attributes:

- **PullType:** The type of request the message refers to.
- **Optional Attributes:**
 - **DiscoveryProfiles:** ServiceProfile requested by the originator of the request.
 - **PayloadSelector:** Filters to be considered on the message payload.
 - **Requests:** Service Capability attributes requested by the originator of the request.
 - **ResponseTimeOut:** The expected time limit for answering to the request.

Table 6.3.3.3-1 illustrates the data structure supported by the PullRequest.

Table 6.3.3.3-1: Data structure of PullRequest

Field Name	Data Type	Note
DiscoveryProfiles	ServiceProfileType	Ref.to [ser-SER-003]
PayloadSelector	PayloadSelectorType	
PullType	PullType	
ResponseTimeOut	Integer	Time in seconds
Requests	ServiceCapabilityType	Ref.to [ser-SER-004]

[Ser-PRQ-002] The PullType shall support the following values:

- GetSubscribers.
- Discover.
- Request.
- Subscribe.
- Unsubscribe.

[Ser-PRQ-003] The PayloadSelectorType shall define the following attributes:

- **Selectors:** List of selection conditions.

Table 6.3.3.3-2 illustrates the data structure supported by the Selectors.

Table 6.3.3.3-2: Data structure of PayloadSelector

Field Name	Data Type	Note
Selectors	SelectorsType	

[Ser-PRQ-004] The SelectorsType shall define the following attributes:

- **Selector:** the expression that allows the selection of the XML elements in the payload.
- **Operator:** the condition operator to be applied to the selector.

Table 6.3.3.3-3 illustrates the data structure supported by the Selectors.

Table 6.3.3.3-3: Data structure of Selectors

Field Name	Data Type	Note
Selector	String	XPATH expression
Operator	ConditionOperatorType	

[Ser-PRQ-005] The ConditionOperatorType shall support the following values:

- Equal.
- Not_Equal.
- Like.
- Not_Like.
- Is_Null.
- Greater_Than.
- Greater_Than_Or_Equal_To.

- Less_Than.
- Less_Than_Or_Equal_To.

6.3.3.4 PullResponse

[Ser-PRS-001] The PullResponse message extension shall define the following attributes:

- **ErrorDetail:** a textual description of the error occurred during the process of preparing the pull response.
- **ResponseCode:** a code representing the result of the pull response.
- **Fulfil:** the criteria adopted to prepare the pull response.

Table 6.3.3.4-1 illustrates the data structure supported by the PullResponse.

Table 6.3.3.4-1: Data structure of PullResponse

Field Name	Data Type	Note
ErrorDetail	String	
Fulfil	ServiceCapabilityType	Ref.to [ser-SER-004]
ResponseCode	ResponseCodeType	

[Ser-PRS-002] The ResultCode shall support the following values:

- Success.
- EndPointNotFound.
- SecurityError.
- InternalGatewayFault.
- InvalidRequestObject.
- Unauthorized.
- BadRequest.
- ServiceTypeNotSupported.
- EntityTypeNotAccepted.
- ObjectTypeNotAccepted.
- ServerError.
- TimestampError.
- AuthenticationError.

6.3.3.5 Push

[Ser-PUS-001] The Push message extension shall define the following attributes:

- **DiscoveryProfiles:** ServiceProfileType requested by the originator of the request.

The ServiceProfile Type is described in clause 6.2 requirement [Ser-SER-003].

6.4 The Participant Class

6.4.1 Participant Class General Requirements

[Ser-PAR-001] A CISE participant shall be described by means of:

- **Description:** A string with a free textual description of the participant.
- **EndpointUrl:** a string defining the url of the participant's adaptor.
- **ID:** This is the unique ID of the participant.
- **Name:** A string with a free textual description of the participant's name.
- **Owner:** A string with a free textual description of the participant's owner.
- **ProvidedServicesIDs:** a string reporting the unique ID of the services provided by the participant.
- **PontOfContact:** contact details of the participant's point of contact.
- **Gateway:** details about the CISE Node the participant belong to.
- **Endpoint:** information about the protocol used by the participant's adaptor.
- **Function:** The mission covered by the participant.
- **Country:** The country of the participant.
- **SeaBasin:** The sea basin of interest of the participant.
- **ClassificationLevel:** The classification level of the information handled by the participant.
- **Community:** One of the 7 user communities participating to CISE.

Figure 6.4.1-1 illustrates the Participant class.

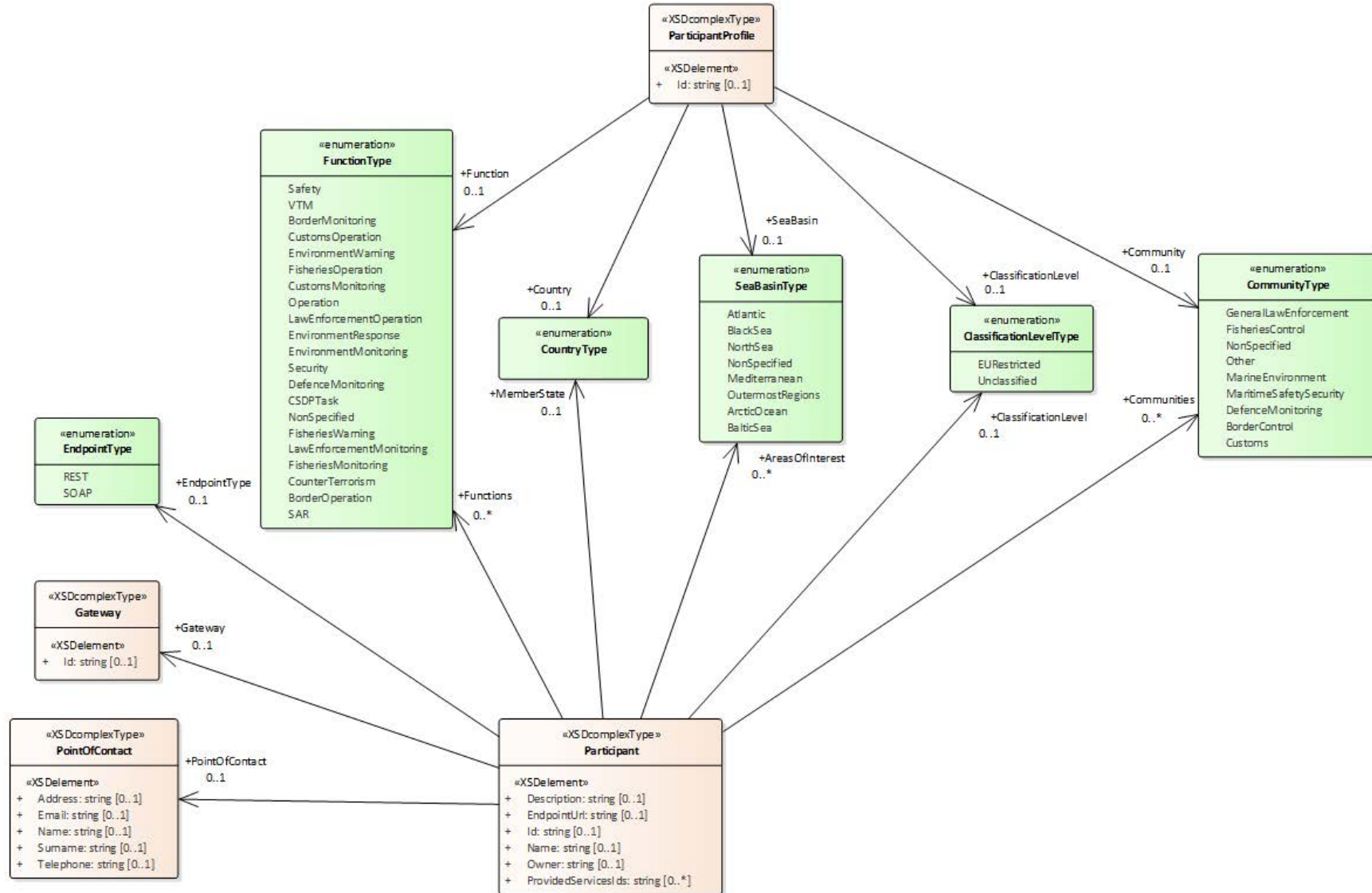


Figure 6.4.1-1: The Participant class model (Source: [i.7])

Table 6.4.1-1 illustrates the data structure supported by the Participant class.

Table 6.4.1-1: Data structure of Participant class

Field Name	Data Type	Note
Description	String	
EndpointUrl	String	
ID	String	UUID
Name	String	
Owner	String	
ProvidedServicesID	String	UUID
PointOfContact	PointOfContactType	
Gateway	GatewayType	
Endpoint	EndpointType	
Function	FunctionType	ref. to [ser-SER-007]
Country	CountryType	ref. to [ser-SER-005]
SeaBasin	SeaBasinType	ref. to [ser-SER-008]
ClassificationLevel	ClassificationLevelType	
Community	CommunityType	ref. to [ser-SER-004]

6.4.2 Enumeration

[Ser-PAR-002] The PointOfContactType shall support the following attributes:

- **Address:** a string consisting of a free textual description of the participant point of contact's address.
- **E-Mail:** a string consisting of a free textual description of the participant point of contact's e-mail.
- **Name:** a string consisting of a free textual description of the participant point of contact's name.
- **Surname:** a string consisting of a free textual description of the participant point of contact's surname.
- **Telephone:** a string consisting of a free textual description of the participant point of contact's telephone.

[Ser-PAR-003] The GatewayType shall support the following attributes:

- **GatewayID:** a string reporting the unique ID of the CISE Node the participant belongs to.

[Ser-PAR-003] The EndpointType shall support the following values:

- REST.
- UNUSED.

[Ser-PAR-004] The ClassificationType shall support the following values:

- EURestricted.
- Unclassified.

6.5 Message Signature

6.5.1 General Requirements

[Ser-SIG-001] A CISE adaptor shall sign all the messages that sends to the CISE Node it belongs to.

[Ser-SIG-002] The signature of a CISE message shall respect the following standards:

- XML Signature Syntax and Processing element namespace [5].
- Canonicalization Method: INCLUSIVE [6].

- Transformation : ENVELOPED [6].
- Signature method: RSA_SHA256 [4].
- Digest method: SHA256 [6].
- Signature key: X.509 certificate [3].

[Ser-SIG-003] Before signing a CISE message, the adaptor shall remove any namespace that could exist in the payload of the message.

Annex A (informative): Change History

Date	Version	Information about changes
September 2021	1.0.0	First Publication
July 2024	1.1.1	Protocol semantics have been updated in order to ensure harmonization and removal of duplications and multiplicities. Formal methodology for requirements specification has been adopted. ETSI guidances and recommendations for service model specification have been followed.

History

Document history		
V1.0.0	September 2021	Publication
V1.1.1	July 2024	Publication