CISE Architecture

The content of this document has been filtered intentionally to remove sensitive information.

1 The CISE Hybrid Architecture

The CISE Hybrid Architecture describes how the Maritime CISE works and how information is exchanged.

The architecture defines the top-level principles and requirements for information exchange and a set of common building blocks and the possible organisational structures for CISE. The hybrid architecture does not impose an organisational structure to the stakeholders, i.e., Member States/EU agencies, but each participant can choose how to share or have access to information.

1.1 Key Principles

The Maritime CISE is driven by the five key principles. These principles were defined in the CISE Hybrid Architecture and further refined within the CISE projects:

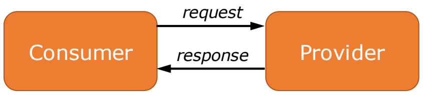
- CISE connects public authorities in the EU and EEA responsible for maritime surveillance: civil and military, regional/sectorial organisations and EU agencies.
- CISE connects existing maritime surveillance systems: not a new surveillance system, not a new screen.
- CISE promotes a sector-neutral solution: 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.

1.2 Communication patterns for information exchange

Five communication patterns describe how the CISE stakeholders can interact to exchange information (between the computer systems). The choice among them will depend on the operational context.

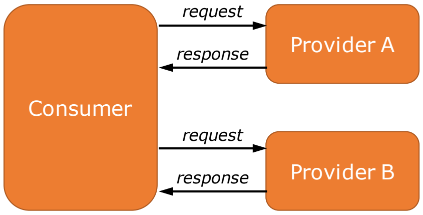
1.2.1 Pull

In this pattern, the consumer knows the exact provider and asks for the information, which is made available only if and when possible (asynchronous).



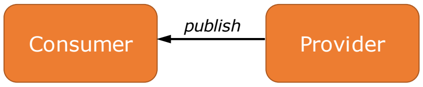
1.2.2 Pull Unknown

The consumer needs some information but does not know who could provide it. Therefore, the consumer asks for the information to all the possible providers. The information is made available (asynchronous) only if and when possible by one or several providers.



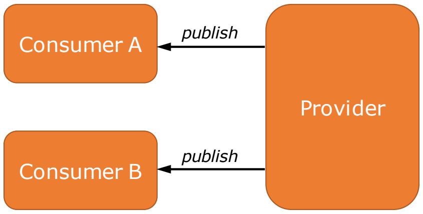
1.2.3 Push

In this pattern, the provider knows a consumer possibly interested in some information and sends this information to the consumer (synchronous).



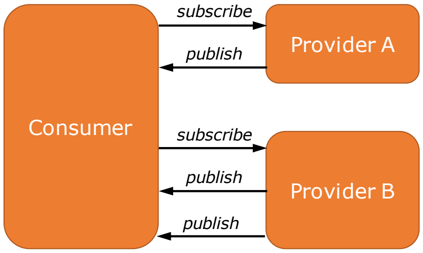
1.2.4 Push Unknown

The provider does not know who could need the information, but the provider sends it (synchronous) to all the possible consumers of a certain profile (within a particular country, sector, etc.)



1.2.5 Publish/Subscribe

In this communication pattern, 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.



1.3 Building blocks and responsibilities

The CISE Hybrid Architecture defined a set of building blocks that should be used in CISE to enable the information exchange between partners:

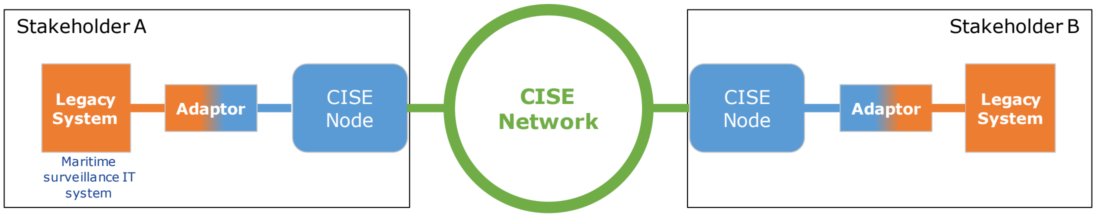


Figure 1. Main building blocks of the CISE Hybrid Architecture.

- **CISE Node:** The CISE Node manages the communication protocol among participants, including the security, access control to the information and the reliability aspects. The CISE Node is a common block for all the partners connected to the network, but the management is not centralised. It uses the CISE Data and Service Models to ensure technical and semantic interoperability among the CISE stakeholders.

  The CISE Node includes the following modules:

  - Service Registry: Distributed directory of metadata about the CISE information services, their status and capabilities, as well as the contact details of the information providers. Each CISE Node manages the metadata of its own services and shares it with the other CISE Nodes.
  - Collaborative service platform: set of tools for virtual collaboration, including audio and video communication, instant messaging, etc.
  - Auditing and monitoring services. These services monitor the activity and performance of the CISE Node and provides statistics to the node owner.

- **Adaptor:** Adaptors translate the CISE data and service model into the specific formats and communication protocols used by the legacy system. The component is specific for each Legacy System, but it could be used to access services provided by different stakeholders.

- **Legacy System[1]:** A Legacy System (LS) represents an existing ICT system owned by a stakeholder and used for maritime surveillance. The system can hold information that could be exchanged through CISE. A LS could also be a national, regional or European Node already gathering information from different other Legacy Systems.

1.4 Organisational Structures

In the CISE Hybrid Architecture, each stakeholder can choose how to share or have access to information. This decision will depend on the internal organisation of the stakeholder and/or the national architecture for information exchange Member State. The following organisational structures are envisioned:

A. Direct connection to the CISE Network

Legacy systems can be connected directly to the CISE network and thus provide and consume information. The stakeholders could connect a single legacy system to the network using a CISE node (hosted and managed by the owner of the legacy system) as shown in Figure 2.

[1] In EUCISE2020, adaptors/legacy systems were called "participants".

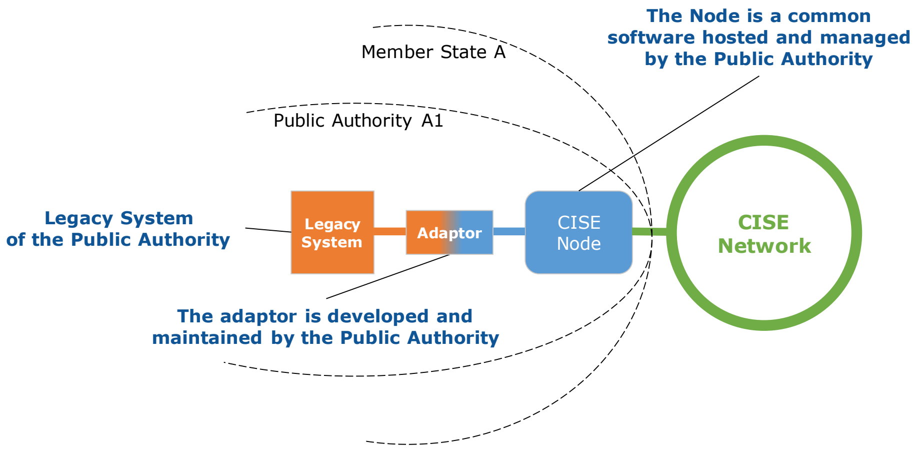

Member State A
Public Authority A1
The Node is a common software hosted and managed by the Public Authority
Legacy System of the Public Authority
Legacy System
Adaptor
CISE Node
CISE Network
The adaptor is developed and maintained by the Public Authority

Figure 2. Legacy system directly connected to the CISE network.

If a stakeholder manages several Legacy Systems (for instance, linked to different business processes), they can be connected to the same CISE Node. The Node can also handle the information exchange and access rights in the communication between the Legacy Systems.

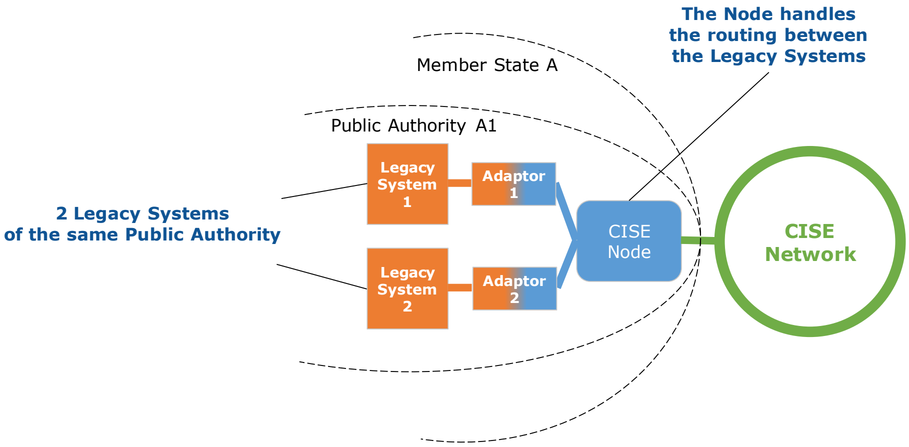


Figure 3. Two legacy systems directly connected to the CISE network using a single node.

B. Direct connection to the CISE Network using a shared CISE Node.

Stakeholders can share a CISE node to connect their legacy systems to the CISE network. In this case, the CISE node will be managed by one of the stakeholders.

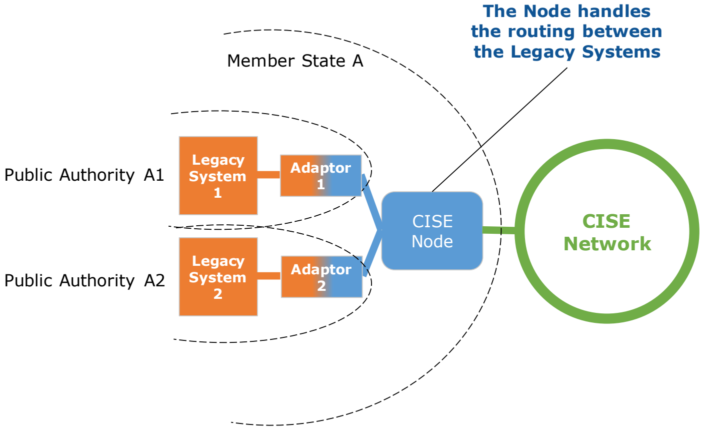


Figure 4. Legacy systems using a shared CISE node to connect to the CISE Network.

C. Connection through a National Node

Stakeholders could connect their legacy systems through a national node (i.e., an IT system in the Member States that redirect messages or may consolidate the information in its own database). National nodes could apply their own access control procedures in addition to the CISE Node's. The CISE Node will be managed by one of the stakeholders.

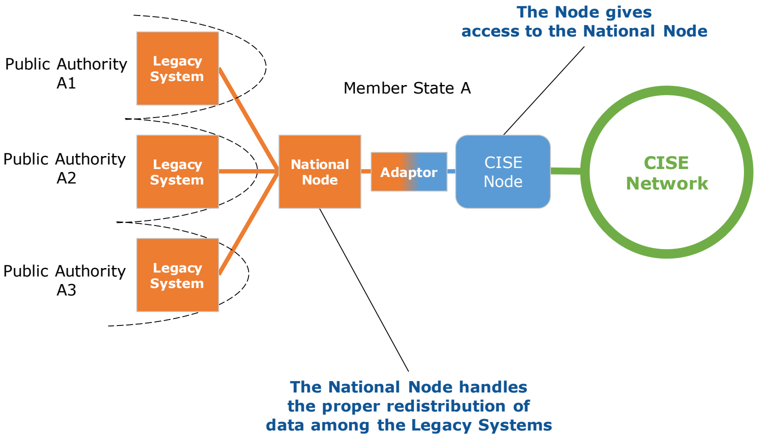


Figure 5. Legacy systems connected through a National Node.

D. Connection through a Regional or a European Node

To benefit from the existing European infrastructures for information exchange, regional and European Nodes can be connected to the CISE Network. Regional and European nodes may exchange their own information or redistribute the information from the legacy systems connected to them. They will enforce the access rights from the information providers.

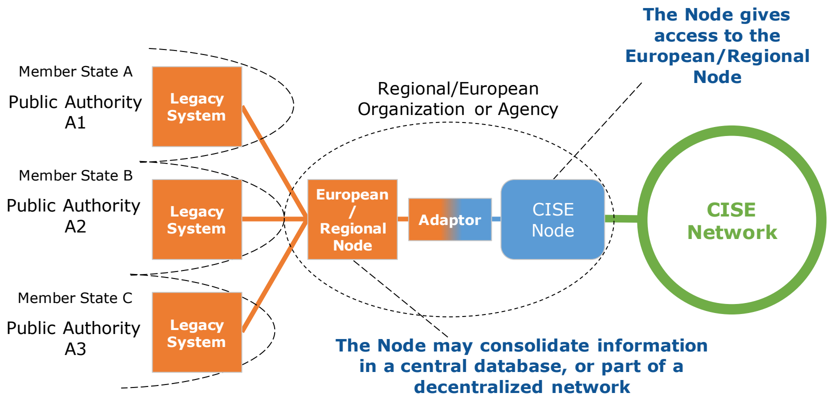


Figure 6. Legacy systems connected through a Regional or a European Node.

1.5 The CISE Interoperability Standards

1.5.1 CISE Data Model

The CISE data model defines the common language for information exchange across sectors and borders. The model is used to represent information that can be exchanged during maritime surveillance operations in which several sectors and/or Member States are involved. Therefore, information specific to a sectoral business case may not be included in the model, or at least not with the same detail level.

The design of the CISE Data model was driven by the following principles:

- sector neutrality (no specific business rules represented);
- flexibility (it should adapt to any context/use);
- extensibility (minimum impact in the maritime surveillance systems in case of extension);
- simplicity and understandability (for domain experts).

The model reuses the existing data standards used in maritime surveillance IT systems in Europe to facilitate the information exchange in the CISE network.

The CISE data model describes the following data entities and the relationships among them: Vessel, Operational Asset, Cargo, Movement, Location, Action, Incident, Anomaly, Risk, Person, Organization and Document.

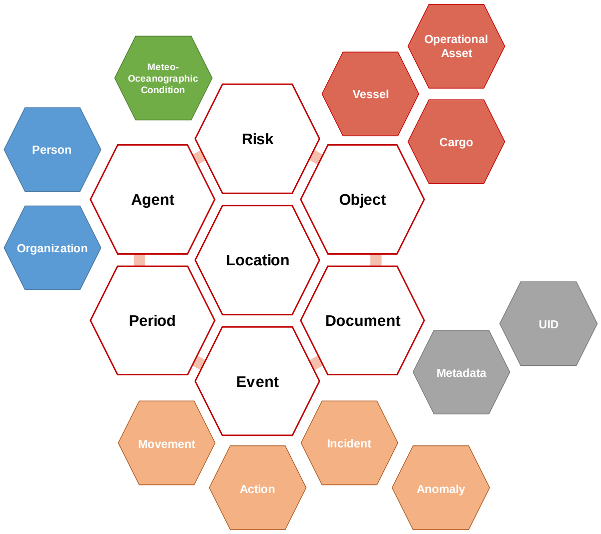
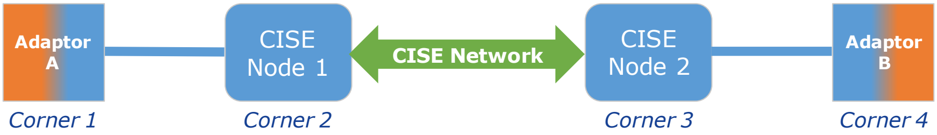


Figure 7. Representation of the main and auxiliary entities in the CISE Data model.

1.5.2 CISE Service Model

The CISE Service model describes the communication protocol between partners' IT systems, based on the five communication patterns. The main features of the communication protocol are the following:

1. The communication protocol follows a four-corner model: LS/Adaptor – Node – Node – LS/Adaptor. Corners 1 and 4 hold the information (information providers/consumers) while corners 2-3 manage the communication.



2. Service-oriented: the communication protocol is oriented to services. Information exchange is implemented using CISE information services:

> *"A CISE information service aims to make available to CISE participants, raw, consolidated or fused data in one or several geographical areas and/or maritime functions. Raw data is considered basic information collected from a source and which has not been subjected to processing or any other manipulation. Consolidated and fused data is considered the collection and integration of data from multiple sources regarding the same data object."* (CISE Hybrid architecture) [2]

With the model, the CISE stakeholders can exchange different information sets using the information services:

- Information collected from any source (e.g., sensors, reporting, etc.) and stored in the Legacy systems. Data exchange directly from sensors is not in the scope of CISE.
- "Added-value" information, resulting from the processing of the collected information (e.g., information filtering, detection of errors in data, anomalies in information, etc.)

[2] In the definition from the Hybrid Architecture, "participant" is a synonym of "stakeholder", "public authority".

Information services offer to the CISE stakeholders a single interface for information exchange in CISE, thus hiding the specificities of the Legacy Systems (e.g., different software, functionalities, etc.)
The Service Model describes how to define and use these CISE information services.

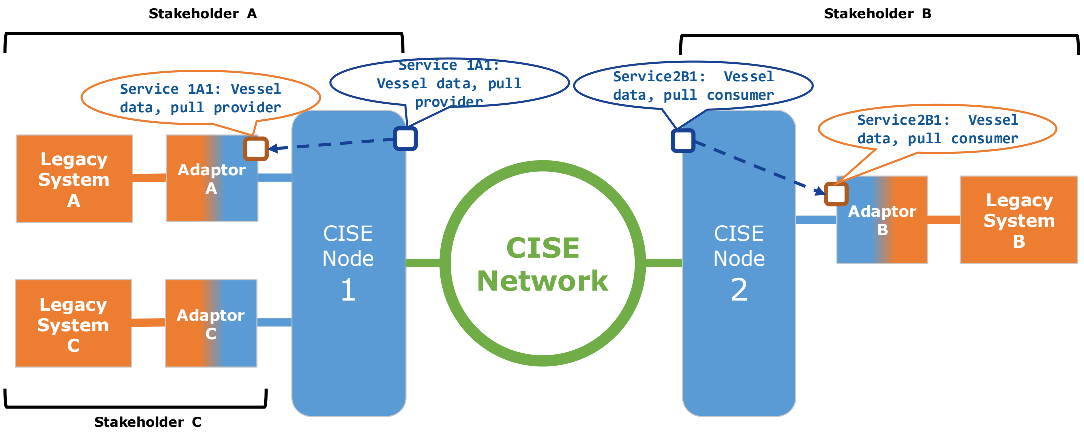
3. Message-driven: the communication protocol is driven by the exchange of messages between the four corners. Messages are the basic piece of data exchanged between two corners. The Service model defines the message flows required to request or receive information to/from the CISE information services using the five communication patterns.

More specifically, the model describes the following aspects:

- Service definition: how to define a CISE information service, metadata used for the description of information services.
- Messaging: message types and message protocol to use information services.
- Service addressing: methods for discovering and invoking the information services provided by each CISE node in the CISE network.
- Access rights: definition of access rights rules for the information services.

1.5.2.1 Service Definition

CISE information services are provided by the adaptors/legacy systems and offered/published in the CISE Node. Providers register their services in the Service Registry (CISE Node), which will help other CISE stakeholders to understand which information is available in the network and what can be expected from the information service.


Stakeholder A
Stakeholder B
Service 1A1: Vessel data, pull provider
Service 1A1: Vessel data, pull provider
Service2B1: Vessel data, pull consumer
Service2B1: Vessel data, pull consumer
Legacy System A
Adaptor A
CISE Node 1
CISE Network
CISE Node 2
Adaptor B
Legacy System B
Legacy System C
Adaptor C
Stakeholder C

Information services are defined by the following metadata:

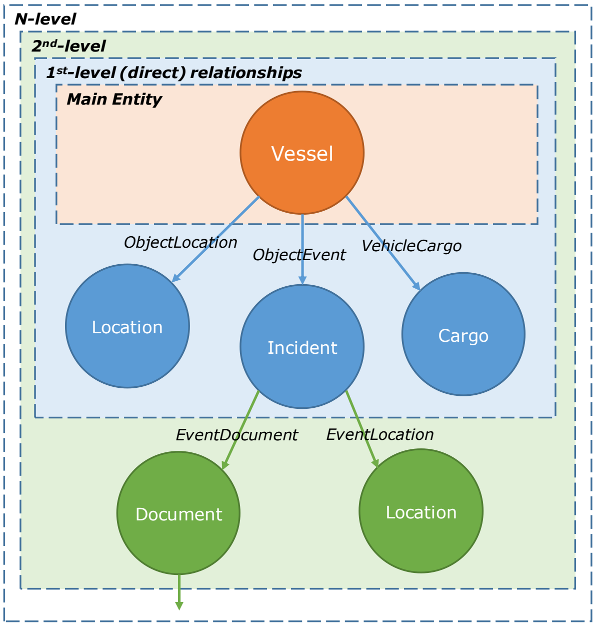
Service ID	Unique identifier of a service in CISE following an agreed scheme (URN), e.g., `eu.cise.authority.vesselService123`. Providers will define the service IDs within the namespace assigned to them.

Service Type

Main data entity exchanged using this service.
For instance, a service of type `VesselService` exchanges vessel data.

Service providers can offer several services of the same service type with different data subsets.
For instance, providers can define one service, type `VesselService`, to exchange information from a vessel database and a second one, type `VesselService`, to exchange vessel information with their location obtained from a sensor.

In each service, providers decide which attributes and related entities will be exchanged (according to the CISE Data Model).
For instance, a service of type `VesselService` will enable the exchange of `Vessel` data entities and could also handle information of the `Cargo`, `Incident`, `Location` data entities (and the corresponding relationships), depending on the service provider and the capabilities of the legacy systems.



Service Operation

Operation supported by the service according to the communication patterns. Possible values.
Possible values: Pull, Push Subscribe, Feedback

Service Role

Role of the service in the information exchange protocol.
Possible values: Consumer, Provider

Service Profile

Metadata describing the features of the information provided by the service:

- Origin (sea basin)
- Data freshness (real-time, historic, etc.)

Service Capabilities

Metadata describing the capabilities of the service:

- subscription capabilities;
- maximum number of concurrent connections;
- maximum delay time to receive a reply.

Service Provider

ID of the Legacy System that offered the service.

Table 1 shows an example of three CISE information services registered in the Service Registry. Figure 8 puts the metadata in the context of the CISE Network.

Table 1. Example of information services.

Service ID	Service Type	Operation	Role	Profile	Capabilities	Service Provider
`eu.nodeA.vessel.pull.consumer.vesselService123`	VesselService	Pull	Consumer		No subscription	eu.systemA
`eu.nodeA.vessel.push.provider.vesselServicer789`	VesselService	Push	Provider	Freshness: Nearly real-time	No subscription	eu.systemC
`eu.nodeB.vessel.pull.provider.vesselService456`	VesselService	Pull	Provider	Freshness: Historic Sea basin: mediterranean	No subscription. Max connections: 10	eu.systemB

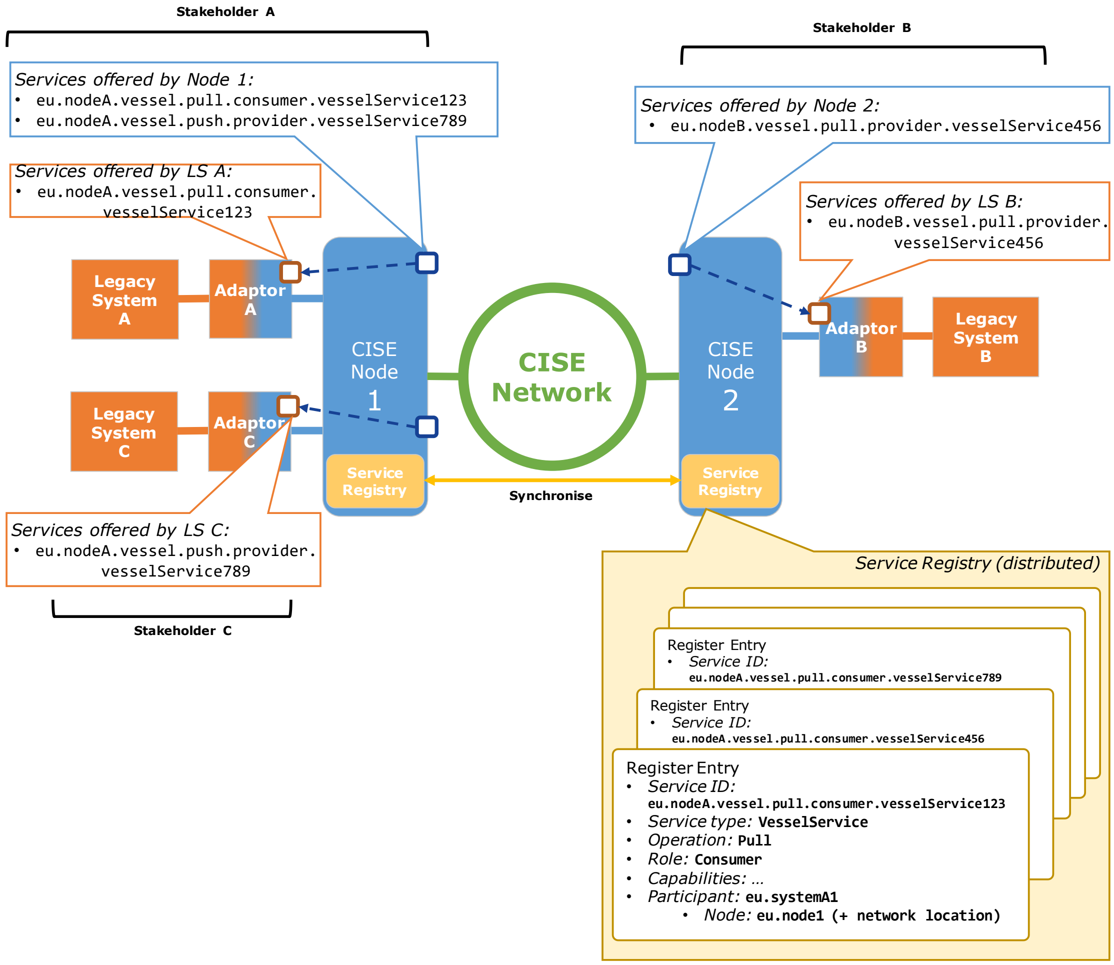

Stakeholder A
Services offered by Node 1:
• eu.nodeA.vessel.pull.consumer.vesselService123
• eu.nodeA.vessel.push.provider.vesselService789
Services offered by LS A:
• eu.nodeA.vessel.pull.consumer.vesselService123
Legacy System A
Adaptor A
Legacy System C
Adaptor C
Services offered by LS C:
• eu.nodeA.vessel.push.provider.vesselService789
Stakeholder C
CISE Node 1
Service Registry
CISE Network
Synchronise
Stakeholder B
Services offered by Node 2:
• eu.nodeB.vessel.pull.provider.vesselService456
Services offered by LS B:
• eu.nodeB.vessel.pull.provider.vesselService456
CISE Node 2
Service Registry
Adaptor B
Legacy System B
Service Registry (distributed)
Register Entry
• Service ID: eu.nodeA.vessel.pull.consumer.vesselService789
Register Entry
• Service ID: eu.nodeA.vessel.pull.consumer.vesselService456
Register Entry
• Service ID: eu.nodeA.vessel.pull.consumer.vesselService123
• Service type: VesselService
• Operation: Pull
• Role: Consumer
• Capabilities: ...
• Participant: eu.systemA1
• Node: eu.node1 (+ network location)

Figure 8. Service metadata in the CISE Network.

1.5.2.2 Messaging

The communication between corners is based on the exchange of messages. Messages are data structures with three main parts:

Message information (or envelop)

It includes information on the message identification, addressing of the message and the action to be performed (the "command").

- Message identification. The following fields are used to define the message identification:
  - MessageID: Unique identifier of the message (UUID): fd5b2bb2-8095-4acf-b6cb-3dd78ba8a572
  - CorrelationID: Needed to reply to another message. Message ID (UUID) of the message that started the communication
  - ContextID: ID (UUID) of the communication. Allows to link several communication flows (for instance to communicate a situation)
- Message addressing. The following fields are used to define the message identification:
  - Sender: Service ID representing the message sender.
  - Recipient: Service ID representing the destination of the message.
  - ccRecipients: List of Service ID indicating the services to which the information has been also sent (informative field, not used for addressing).
- Message action. Messages carry the information to perform a single action of the communication protocol (e.g., request information, provide information, acknowledge reception, etc.) This action is directly related to the communication pattern and encoded in the following message subtypes:
  - PullRequest message:
    - Request information.
    - Subscribe/unsubscribe from a service.
    - Retrieve the service subscribers.
  - PullResponse message: Provide information, after request.
  - Push message: Provide information, with no previous request.
  - Acknowledgement message: confirm message reception. Two types:
    - Synchronous, from "your" node (corner 2), to indicate that the message correct and sent to Corner 3.
    - Asynchronous, from the "other" node (corner 3), to indicate that the message was delivered to Corner 4.
  - Feedback message: communicate feedback on the information exchanged, e.g., an error in the information, a punctual update on an important piece of information, etc.

Message payload

It includes the data exchanged, formatted using the CISE Data Model, and additional meta-information on the payload: data sensitivity, etc. The payload can be encrypted, but the encryption is managed by Corner 1 and 4.

Message signature

Digital signature of the message, which ensures the authenticity of the message sender. The authenticity is checked every hop. The digital signature follows the W3C standard on XML signature (https://www.w3.org/TR/xmldsig-core1/

1.5.2.3 Data Structures

The CISE service model formalises the data structures in three packages:

- Service, describing the metadata related to the information services (Figure 9);
- Message, describing the messages required to invoke an information service, an/or receive information (Figure 10);
- Participant, describing the metadata related to legacy systems/adaptors (Figure 11).

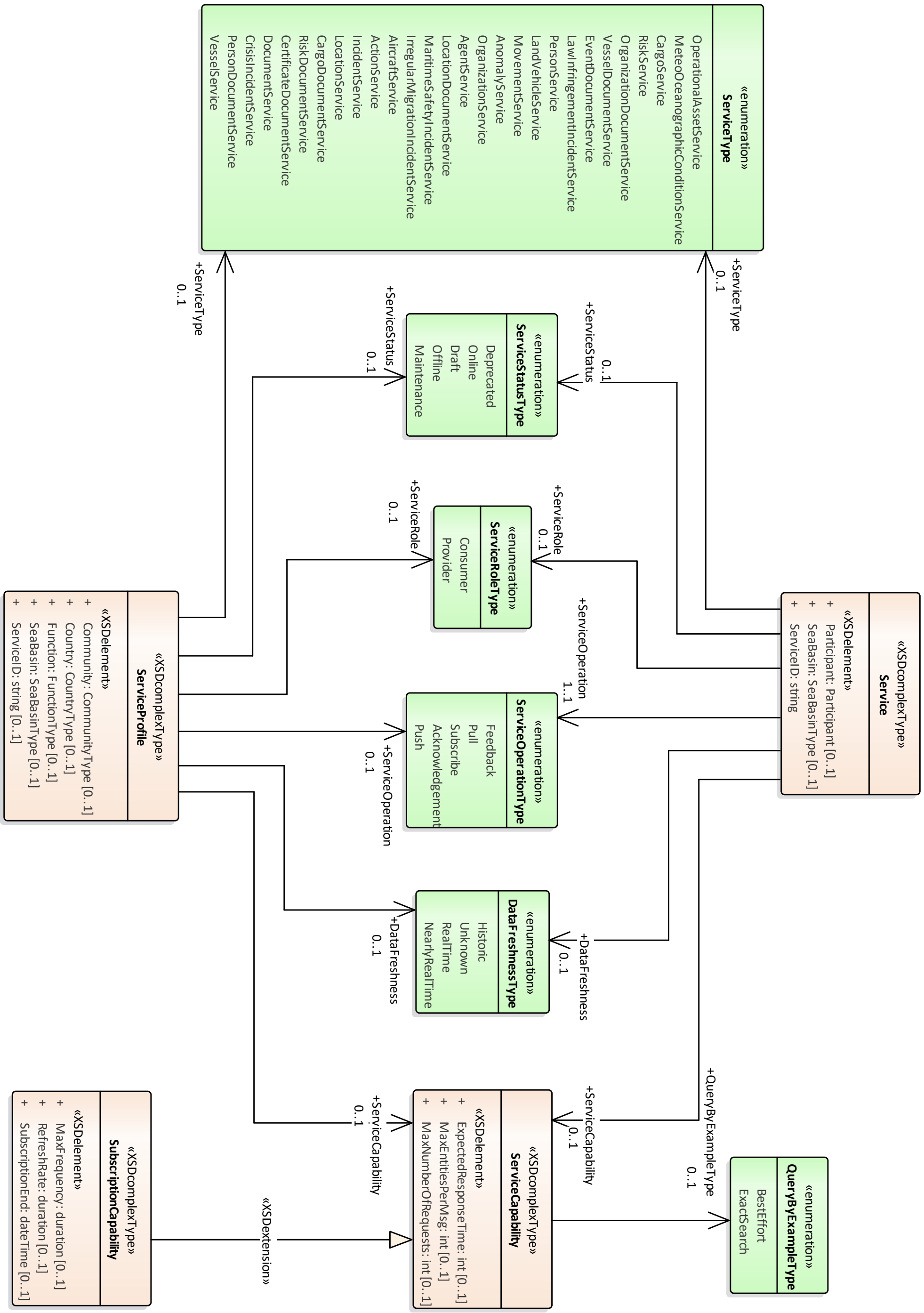


Figure 9. Service metadata – XSD view.

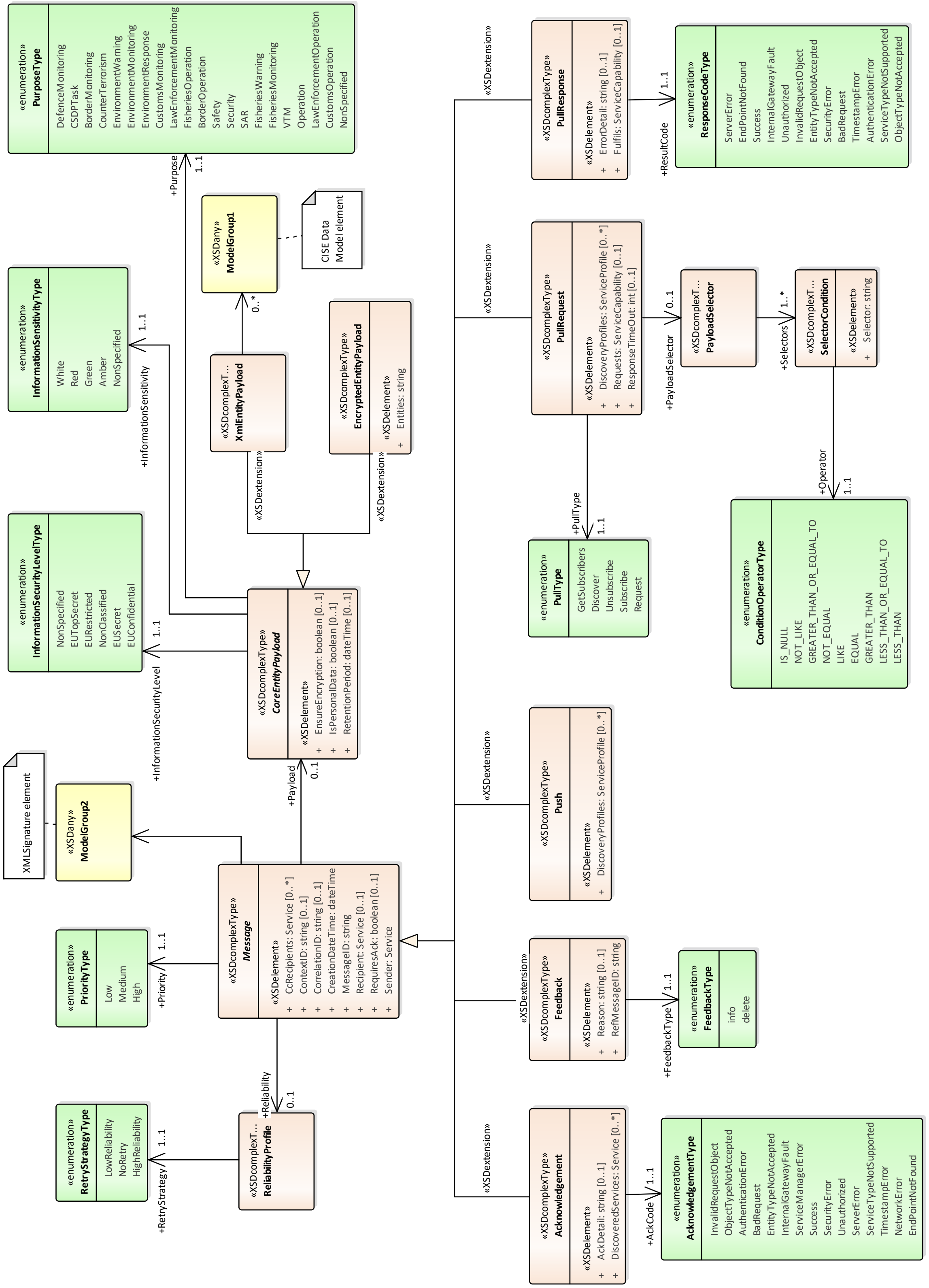


Figure 10. Service metadata – XSD view.

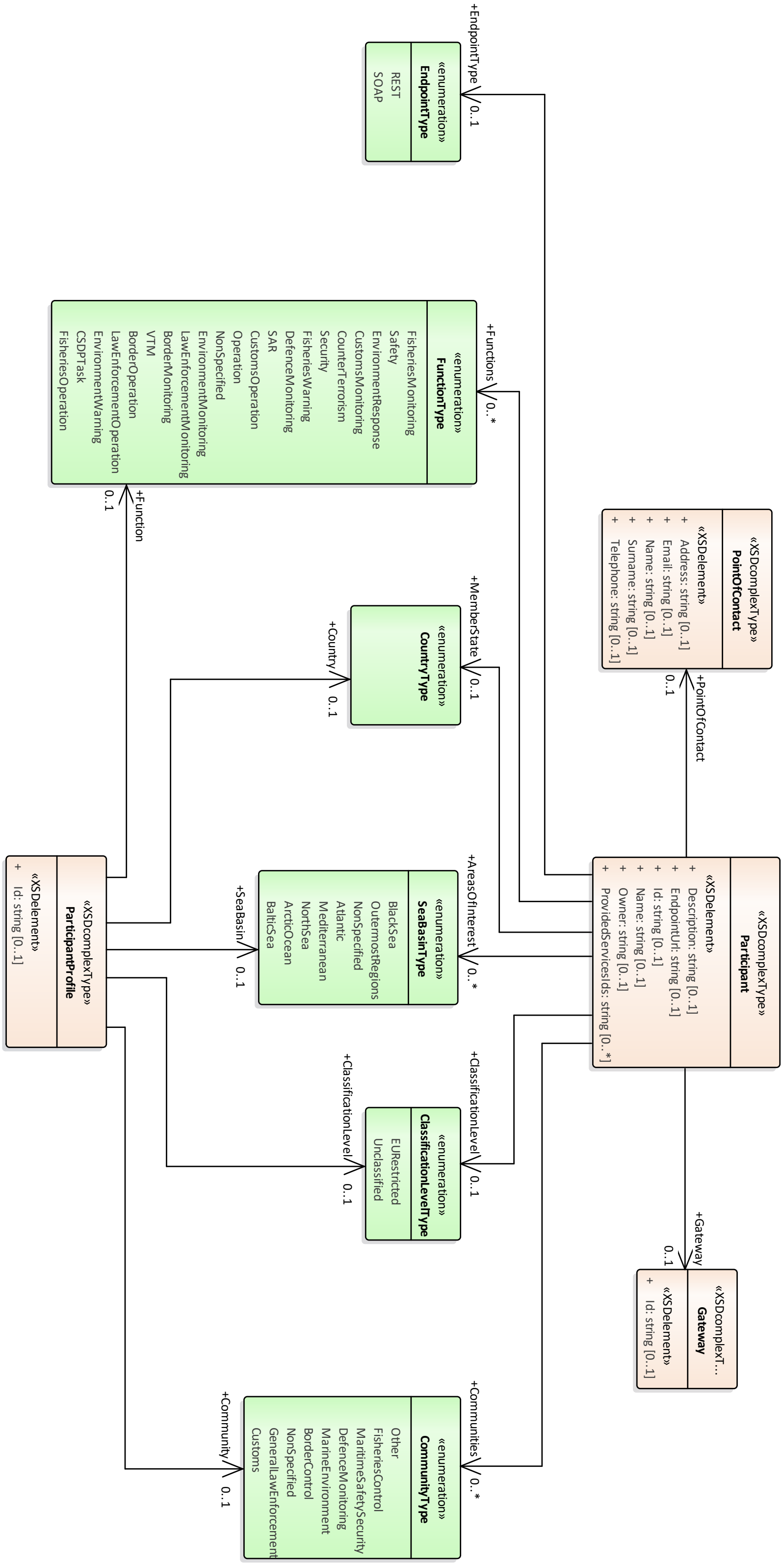


Figure 11. Participant metadata – XSD view.

1.5.2.4 Message flows for the communication patterns

This section describes the message flows required to use the CISE information services following the five communication patterns.

Each pattern requires the use of a sequence of different message types to use the CISE information service. The following table summarises the message types used in each communication pattern.

Message Type	**Communication Pattern**				
	Push	**Push Unknown**	**Pull**	**Pull Unknown**	**Publish/ Subscribe**
Push	×	×			×
PullRequest			×	×	×
PullResponse			×	×	×
Feedback	×	×	×	×	×
Acknowledgement	×	×	×	×	×

1.5.2.4.1 Using information services with the Pull pattern

In this pattern, the CISE consumer requests a piece of information to a CISE information service using the `PullRequest` message. The CISE provider replies using the `PullResponse` message.

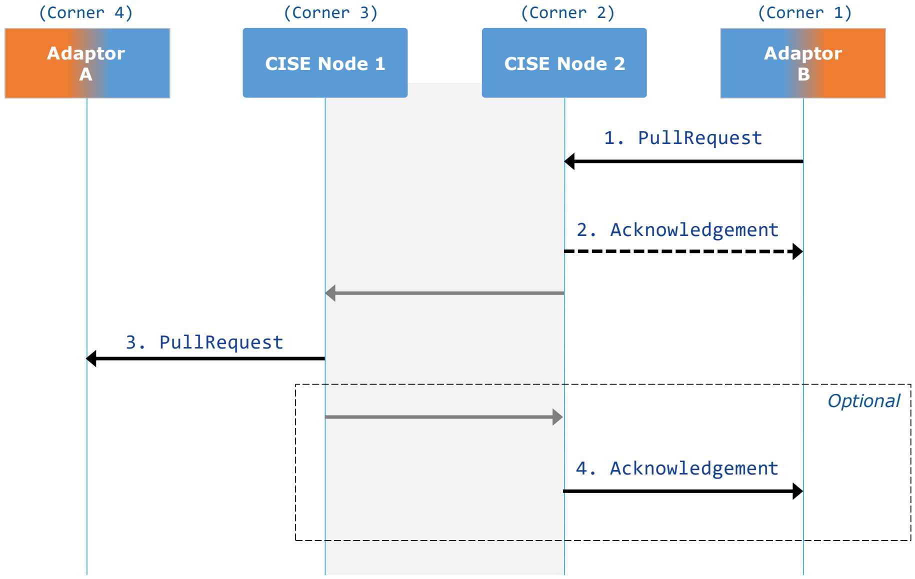
This message flow is used with the services implementing the Pull operation. The flow is divided into two independent processes:

1. Request: Request of information from Corner 1 to Corner 4. The request may contain a query following the Query-by-Example mechanism.
2. Response: Reply with the information requested from Corner 4 to Corner 1.

The following services must be provided to implement the pattern:

- Corner 1-2: service type ServiceTypeA, Pull consumer
- Corner 3-4: service type ServiceTypeA, Pull provider

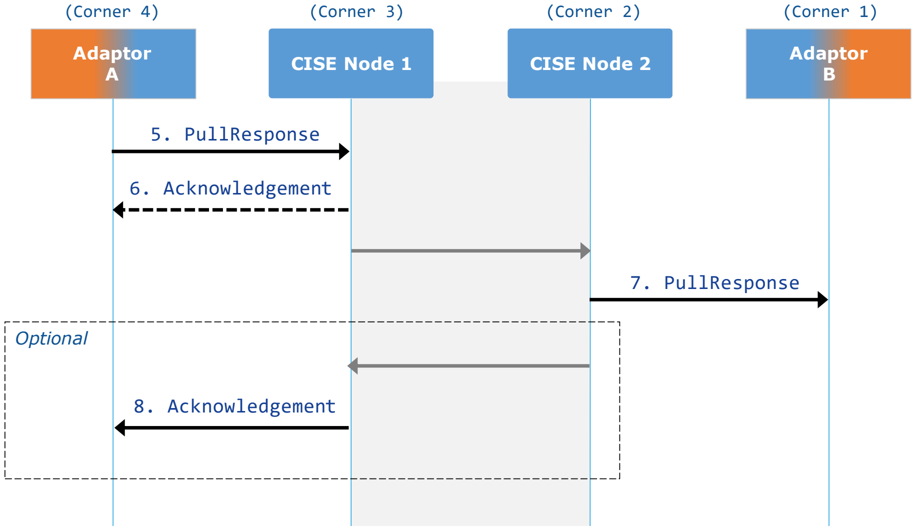
1.5.2.4.1.1 Request information using the PullRequest message



1.5.2.4.1.2 Query-by-example mechanism

To be described.

1.5.2.4.1.3 Provide information after a request using the PullResponse message



1.5.2.4.2 Using information services with the Pull Unknown pattern

The CISE consumer requests a piece of information to a group of CISE providers using the `PullRequest` operation. The CISE Node looks for providers using the Service Registry.

To be described.

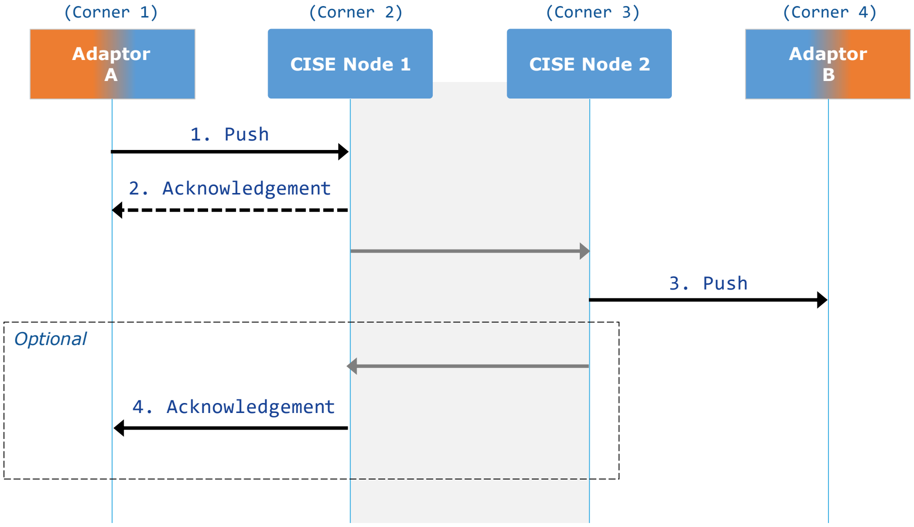
1.5.2.4.3 Using information services with the Push pattern

The CISE provider sends a piece of information to the CISE consumer using the `Push` message.

This message flow is used with the services implementing the Push operation. In this flow, information is provided from Corner 1 to Corner 4 with no initial request (i.e., Corner 4 did not request the information).

The following services must be provided to implement the pattern:

- Corner 1-2: service type ServiceTypeA, Push consumer
- Corner 3-4: service type ServiceType A, Push provider



1.5.2.4.4 Using information services with the Push Unknown pattern

The CISE provider sends a piece of information to a group of CISE consumers (who might be interested in it) using the `Push` message. The CISE Node looks for consumers using the CISE Service Registry.

To be described.

1.5.2.4.5 Using the Publish/Subscribe pattern

The CISE consumer subscribes to a piece of information from the CISE Node using the `PullRequest` message. The information provider notifies the new information to the CISE Node, which distributes the information to the subscribers.

To be described.

1.5.2.5 Access rights

The CISE Node stores and enforces the access rights for each CISE information service offered.

When a service is published in the Node, the information provider can define an Access Rights Matrix, which defines a set of access rules per legacy system (participant). The access rules specify whether legacy systems can use and information service and, if so, which information (i.e., main entity’s attributes, relationships) is available. If the information provider does not define the Access Rights Matrix, the access to the information service is denied by default.

The access rights matrix does not have an impact on the adaptor. However, legacy systems or adaptors could also define and enforce their own access rights matrix if needed.

2 The CISE Node

The first version of the CISE Node was developed in the context of the EUCISE 2020 pre-operational validation FP7 project.

The software of this building block enables point-to-point information exchange between their maritime surveillance systems using the CISE interoperability standards. The CISE Node can be used to exchange information in the unclassified CISE Network, but it is not certified for classified networks yet.

2.1 Functionalities

The functionalities implemented in the CISE Node are grouped into the following service categories (Figure 12):

Core Services: infrastructure services that provide common facilities. These services enable the connection of the Legacy Systems through the CISE Network and they ensure the secure data transfer between Legacy Systems. Core services include:

- Network and secure communication services: These services manage the secure message-based communication between the CISE nodes.
- Application security services: These services manage/enforce the application security policy:
  - Identification/Authentication of users
  - Access rights to the information
- Auditing services: The Auditing Services periodically test the availability of the services, resources on a specific configuration.
  - Logging
  - Monitoring
  - Accounting
- Collaborative services: The Collaborative Services facilitate the communications and the work among the maritime surveillance operators: Instant messaging, e-mail, video and voice conference, whiteboard, file transfer, shared document repository and shared calendar.
- Administration console: The Administration Console enables the logged user to see the status of all provided services; manage credentials (add, delete, modify); manage authorisation rules (add, delete, modify) for each Common service; manage services (add, delete, update); see statistics about the services; see and manage the log; create reports on the provided statistics.

Common Services: application services that provide the capability to exchange data in the EUCISE2020 Network. Consequently, these services manage EUCISE2020 data model entities.

Advanced Services, which compose and orchestrate Common services to implement added-value functionalities. ***Advance services are out of the scope of the CISE Transitional Phase.***

- Vessel Fusion and Association: Responsible to exchange vessel track data using the Common Services and to fuse track information when required.
- Light Client: GIS Web interface to visualise the information exchanged through the Common Services.

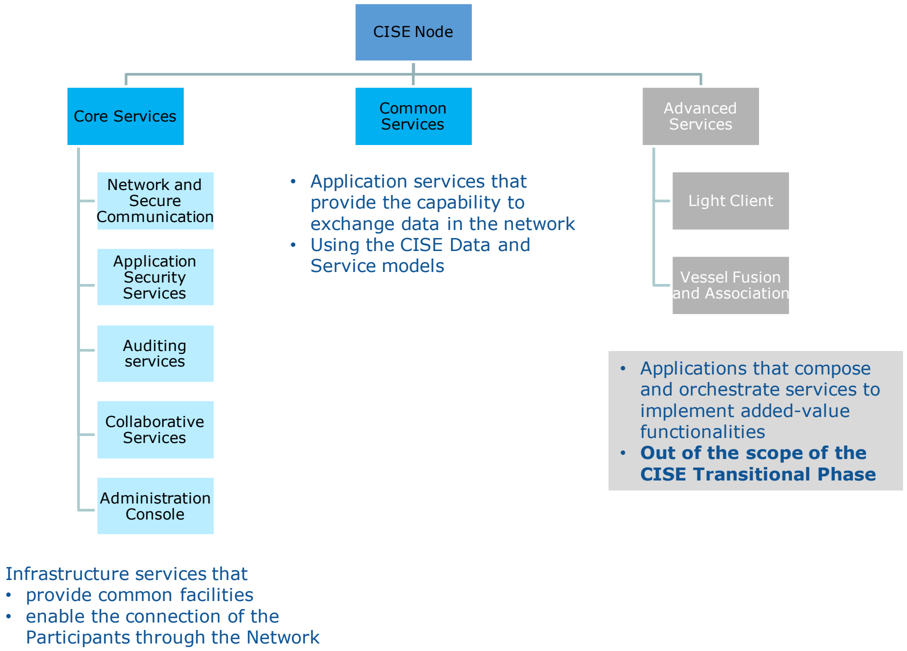

CISE Node
Core Services
Common Services
Advanced Services
Network and Secure Communication
Application Security Services
Auditing services
Collaborative Services
Administration Console
Application services that provide the capability to exchange data in the network
Using the CISE Data and Service models
Light Client
Vessel Fusion and Association
Applications that compose and orchestrate services to implement added-value functionalities
Out of the scope of the CISE Transitional Phase
Infrastructure services that
provide common facilities
enable the connection of the Participants through the Network

Figure 12. Functionalities of the CISE Node.

2.2 Node Configurations

The CISE Node can be deployed in three configurations, namely A, B and C, with different functionalities and hardware requirements.

The possible configurations are the following:

Table 2. Configurations of the CISE Node.

Configuration	Functionalities	Number of Legacy systems/Adaptors	Hardware requirements
Node type A	Core, Common services	1	+
Node type B	Core, Common services	N	+
Node type C	Core, Common and Advanced Services	N	++
High-Availability features	Features for High Availability for Node type B, C	N	+++

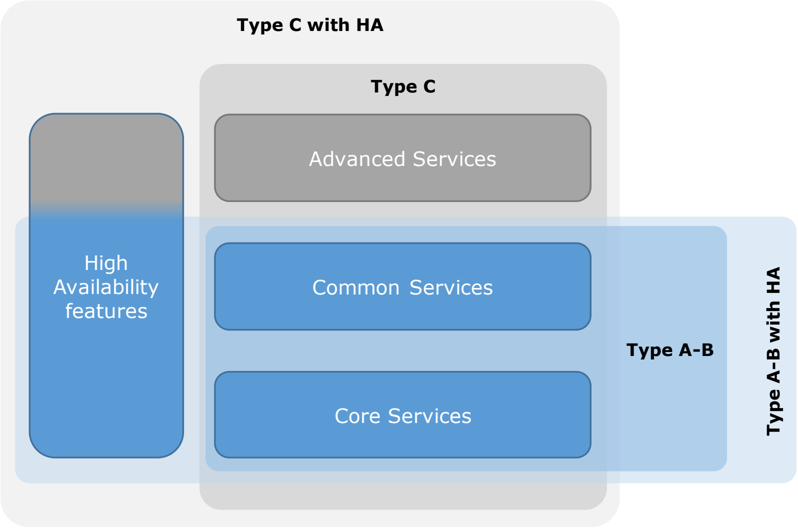


Figure 13. Node configurations and services.

Additional information:

- **Node type C is out of the scope of the CISE Transitional Phase.**
- At technical level, there is no difference between Node type A and type B.
- For a more detailed description of the Hardware requirements, please refer to Section 2.4.2.4.

2.3 External Interfaces of the CISE Node

The CISE Node exposes two external interfaces (Figure 14):

1. The **Node-Node interface**: communication interface between Nodes, managed by the Network and Secure Communication services (Core services). This interface enables the communication using the JMS message and CISE messages (i.e., defined in the CISE Service Model).

2. The **Adaptor-Node** interface: communication between Adaptor and Node, managed by the Common Services. This interface enables the communication using the CISE Service model protocol. All the communication is based on the exchange of CISE messages using the web service CISEMessageService (the service signature can be found in Annex X).

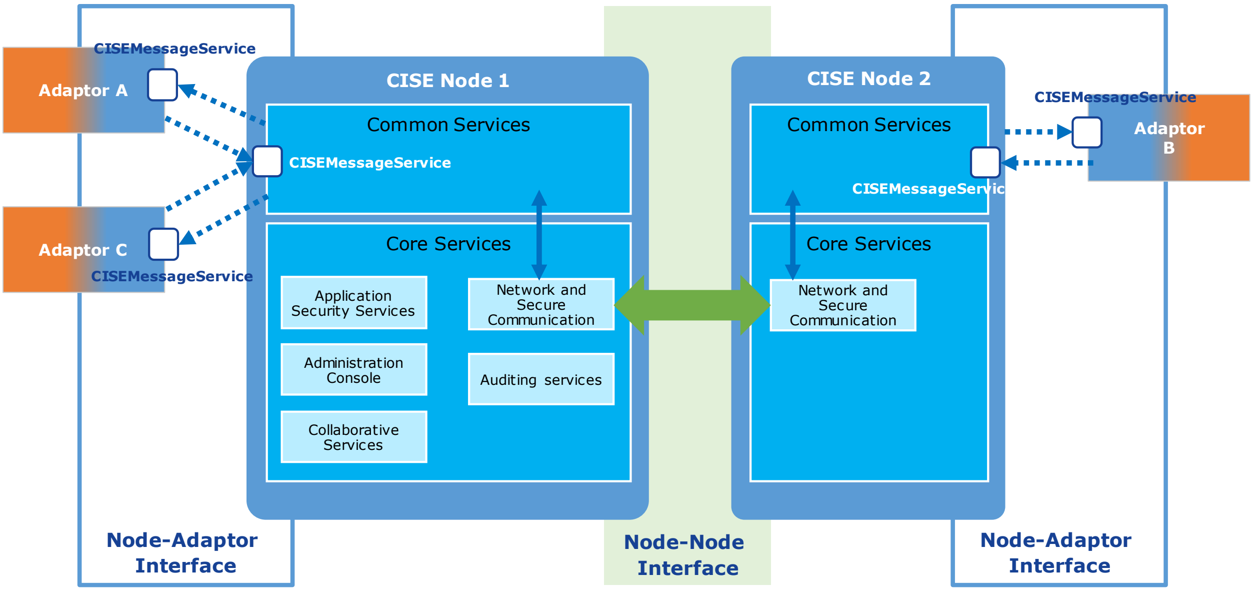


Figure 14. External interfaces of the CISE Node.

2.4 Node Architecture

The functionalities of the CISE Node are implemented in several software components, which are deployed across several virtual machines in the same virtual network.

2.4.1 Logical Architecture

The functionalities of the CISE Node (Core and Common services) were developed in a set of software components, supported by several subsystems, using Java technologies. Figure 15 describes the logical architecture of the CISE Node, including the different software components and the dependencies among them. For a brief description of each component, please check Table 3.

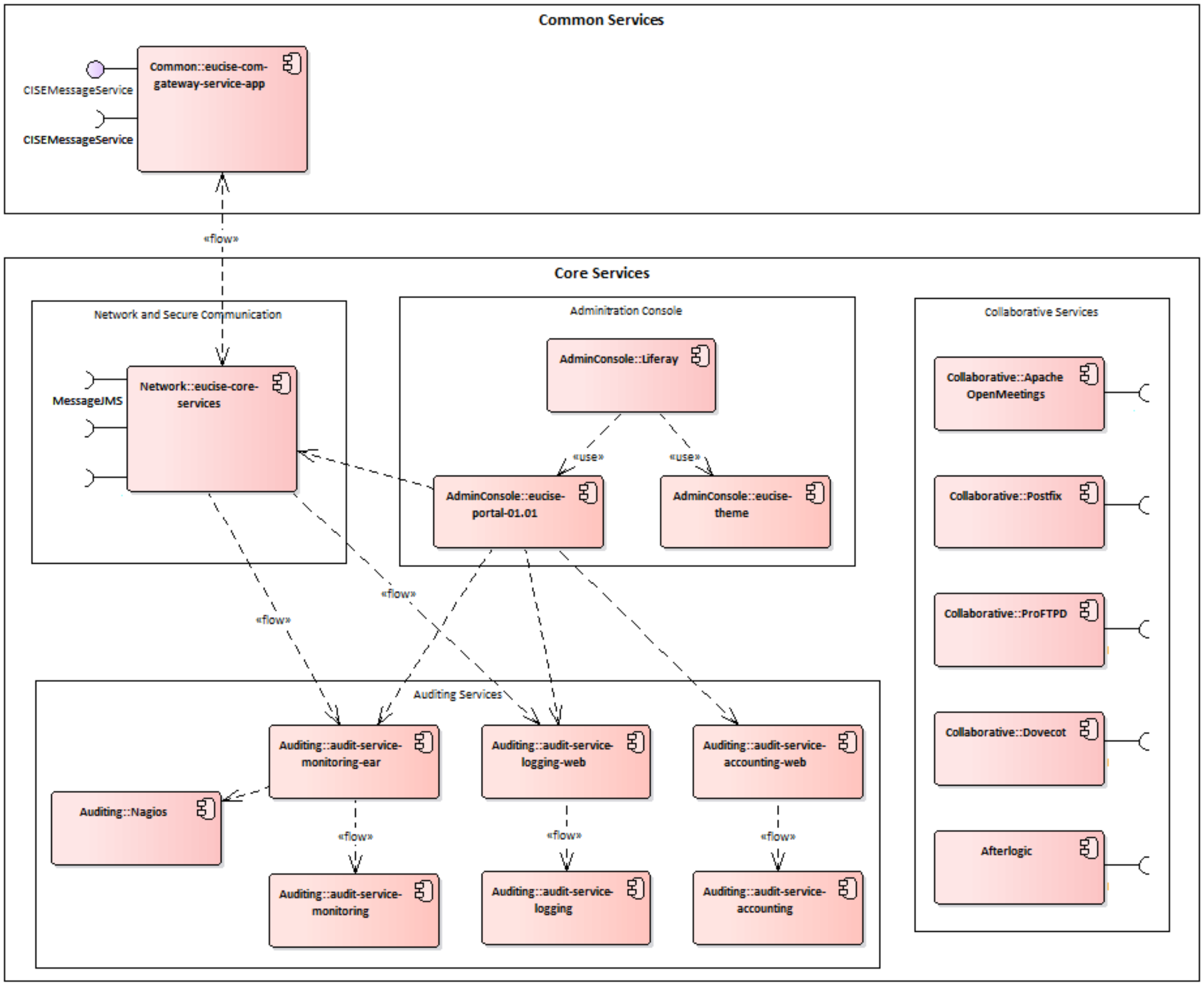

Common Services
CISEMessageService
CISEMessageService
Common::eucise-com-gateway-service-app
«flow»
Core Services
Network and Secure Communication
MessageJMS
Network::eucise-core-services
Adminitration Console
AdminConsole::Liferay
«use»
«use»
AdminConsole::eucise-portal-01.01
AdminConsole::eucise-theme
«flow»
«flow»
Collaborative Services
Collaborative::Apache OpenMeetings
Collaborative::Postfix
Collaborative::ProFTPD
Collaborative::Dovecot
Afterlogic
Auditing Services
Auditing::audit-service-monitoring-ear
Auditing::audit-service-logging-web
Auditing::audit-service-accounting-web
Auditing::Nagios
«flow»
«flow»
«flow»
Auditing::audit-service-monitoring
Auditing::audit-service-logging
Auditing::audit-service-accounting

Figure 15. Logical architecture of the CISE Node (component view).

Table 3. Software components of the CISE Node (type A-B).

Package	Software component	Description
Core services	eucise-core-services	Core Services software interface Requires a connection to a JMS, Consul and LDAP.
	Liferay	Lifeway instance holding the Administration Console
	eucise-portal-01.01	Administration console: Liferay plugin
	eucise-theme	Liferay style for the Administration Console
	audit-service-accounting-web	Auditing Services, Accounting – Web interface
	audit-service-accounting	Auditing Services, Accounting
	audit-service-logging-web	Auditing Services, Logging – Web interface
	audit-service-logging	Auditing Services, Logging
	audit-service-monitoring-ear	Auditing Services, Monitoring – Web interface
	audit-service-monitoring	Auditing Services, Monitoring
	Apache OpenMeetings	Collaborative services: Apache OpenMeetings suite Requires a connection to LDAP
	Postfix	Collaborative services: IMAP server Requires a connection to LDAP

	Dovecot	Collaborative services: SMTP server Requires a connection to LDAP
	ProFTPD	Collaborative services: FTP server Requires a connection to LDAP
	Afterlogic	Collaborative services: Webmail client Requires a connection to LDAP
Core services	eucise-com-gateway-service-app	Common Services software interface

The following third-party components were used during the development (open-source components):

```
com.fasterxml.jackson.core.jackson-annotations
com.fasterxml.jackson.core.jackson-core
com.fasterxml.jackson.core.jackson-databind
com.google.code.gson:gson
com.googlecode.concurrentlinkedhashmap.concurrentlinkedhashmap-lru
commons-beanutils.commons-beanutils
commons-codec.commons-codec
commons-io.commons-io
commons-io:commons-io
javax.servlet:javax.servlet-api
javax:javaee-api:7.0
junit.junit
org.apache.activemq.activemq-client
org.apache.activemq.activemq-pool
org.apache.commons.commons-configuration2
org.apache.commons.commons-lang3
org.apache.commons:commons-lang3
org.apache.httpcomponents.httpclient
org.apache.openejb.openejb-core
org.apache.velocity:velocity
org.glassfish.javax.json
org.glassfish:javax.json
org.glassfish:javax.json
org.hibernate.hibernate-core
org.hibernate.hibernate-entitymanager
org.hibernate:hibernate-core
org.hibernate:hibernate-entitymanager
org.jboss.resteasy.resteasy-client
org.jboss.resteasy.resteasy-jackson2-provider
org.jboss.resteasy.resteasy-jaxb-provider
org.jboss.resteasy.resteasy-jaxrs
org.jboss.resteasy:resteasy-client
org.jboss.resteasy:resteasy-jaxrs
org.jvnet.jaxb2_commons.jaxb2-basics
org.mockito:mockito-all
org.quartz-scheduler.quartz
org.quartz-scheduler.quartz-jobs
org.quartz-scheduler:quartz
org.slf4j.slf4j-jcl
org.springframework.boot:spring-boot-starter-security
org.springframework.boot:spring-boot-starter-web
org.springframework.ldap:spring-ldap-core
org.springframework.ldap:spring-ldap-core
org.springframework.security:spring-security-config
org.springframework.security:spring-security-ldap
org.springframework.security:spring-security-ldap
org.springframework.security:spring-security-web
org.springframework:spring-context
org.springframework:spring-context
org.springframework:spring-context-support
org.springframework:spring-context-support
org.springframework:spring-core
org.springframework:spring-core
org.springframework:spring-core
org.springframework:spring-orm
org.springframework:spring-orm
org.springframework:spring-test
org.springframework:spring-test
org.springframework:spring-tx
org.springframework:spring-tx
org.springframework:spring-web
org.springframework:spring-web
org.springframework:spring-webmvc
org.xhtmlrenderer:flying-saucer-pdf-itext5
```

2.4.2 Physical Architecture

The CISE Node is deployed in virtual environment, hosted in the stakeholders' premises. A top-level domain and a specific subnet `0.0.0.0/0` are assigned to the CISE Node before deployment. The instances of the CISE Node in the CISE Network share the address space `0.0.0.0/0`.

2.4.2.1 Virtual Infrastructure - Overview

The CISE node software is deployed in a set of virtual machines that communicate using the internal virtual network. Figure 16 shows a typical deployment of a CISE Node type A-B using the **top-level domain XX** and the **subnet** `0.0.0.0/0`. The virtual machines are in the domain **node.XX**

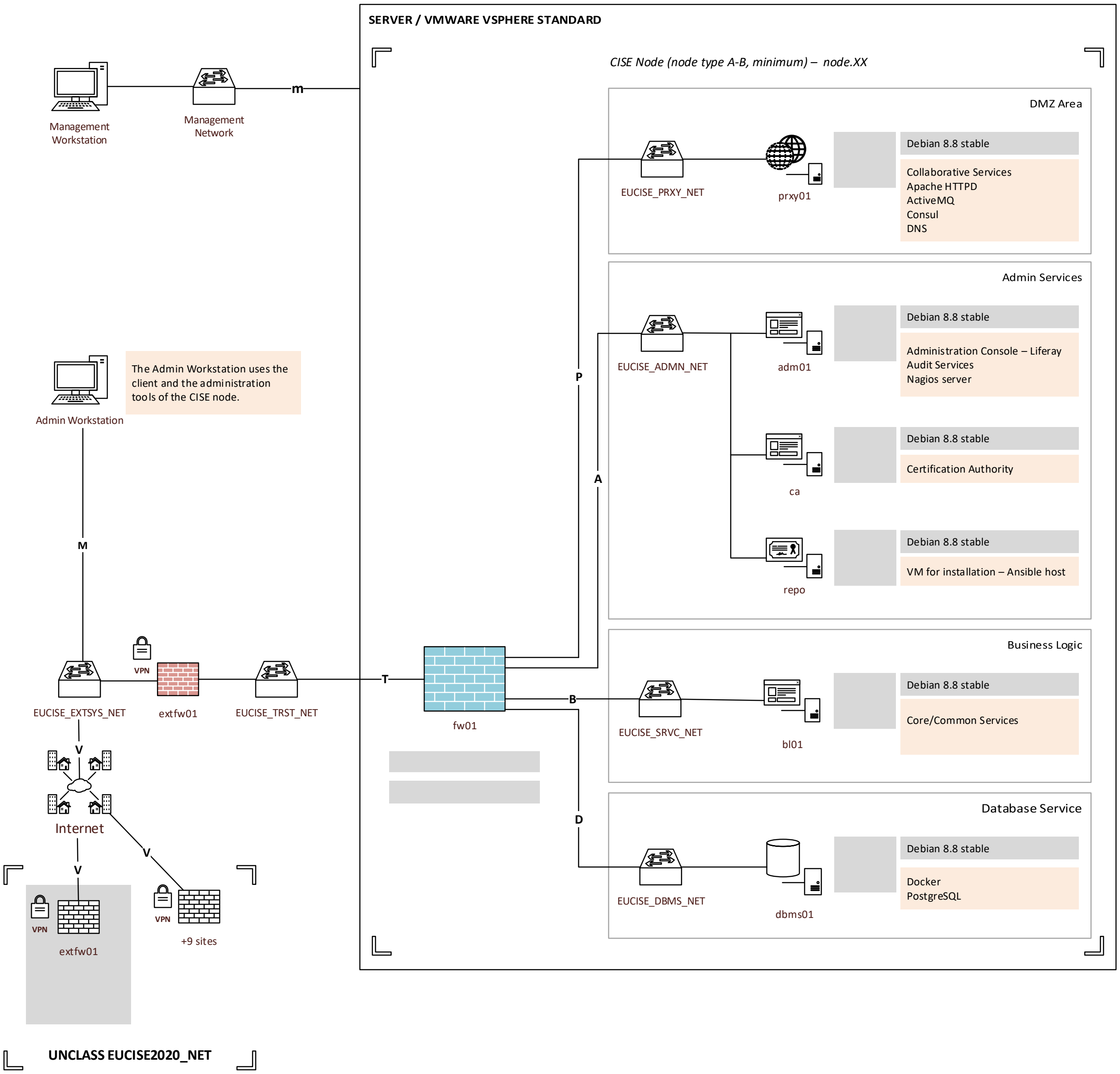


Figure 16. Deployment of the CISE Node.

2.4.2.2 Hypervisor

The core of the virtual infrastructure is the hypervisor, which manages the internal network and the virtual machines. The supported hypervisors for the CISE Node are the following:

- VMWare ESXi (Proprietary) - https://www.vmware.com/uk/products/vsphere.html
- PROXMOX (Open source and free) - https://www.proxmox.com/en/ *(not tested during EUCISE 2020)*

2.4.2.3 Internal Network

The internal network of the CISE Node is provided by the virtual infrastructure of the CISE Node. As depicted in Figure 17, the internal firewall (virtual) controls the communication between the external firewall and the DMZ network (virtual), as well as between the DMZ network and the other subnetworks. The external firewall could be a physical device or a virtual appliance.

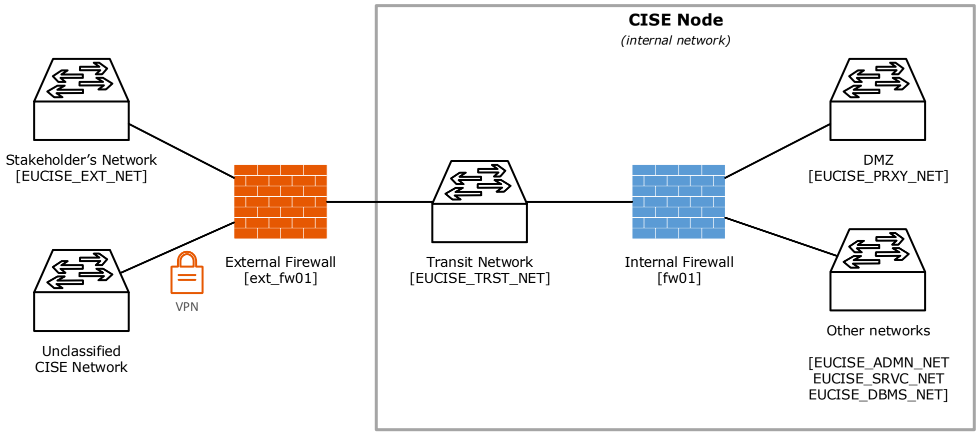


Figure 17. Internal and external firewalls in the CISE Node.

The virtual networks within the CISE Node are described in Table 4 (address space: `0.0.0.0/0`).

Table 4. CISE Node - Internal network.

Network	Name in the Technical Note	Description	Subnet	CIDR	Mask	Broadcast	GW
DMZ	EUCISE_PRXY_NET	DMZ Service Network					
BL	EUCISE_SRVC_NET	Internal Services Network					
Admin	EUCISE_ADMN_NET	Administration Network					
DB	EUCISE_DBMS_NET	Internal Database Network					
Management[3]	EUCISE_MGMT_NET	Management Workstation's network					
Transit	EUCISE_TRST_NET	Network between the internal and the external firewalls	The setup will depend on the stakeholders' network infrastructure.				

2.4.2.4 Virtual Hosts

2.4.2.4.1 Virtual Machine Setup

The setup of the virtual machines for the CISE Node (type A-B) is described in Table 5.

Table 5. CISE Node - Virtual machines.

Hostname (Virtual Machine)	Description	Services	Hardware requirements			OS
			VCPU	RAM (GB)	Disk (GB)	
adm01	Network Services	Audit Services Administration Console				

[3] The Management network can be internal or external to the CISE Node. This section introduced the setup for the internal network.

Hostname (Virtual Machine)	Description	Services	Hardware requirements			OS
			VCPU	RAM (GB)	Disk (GB)	
bl01	Application Layer	Common Services Core Services				Debian 8.8 stable
dbms01	Database	PostgreSQL				Debian 8.8 stable
ca	Certification Authority	Certification Authority				Debian 8.8 stable
fw01	Internal firewall	Routing/Security Time server - NTP				Debian 8.8 stable
prxy01	Application Layer	Collaborative Services Network Service Communication Service DNS LDAP				Debian 8.8 stable
repo	Repository for the installation					Debian 8.8 stable

2.4.2.4.2 Network Setup

Table 6 shows the network configuration for the virtual machines in the internal network.

Table 6. CISE Node - Network setup for the virtual machines.

Hostname	FQDN	Network	IP	Name server	Time server
adm01		Admin			
bl01		BL			
dbms01		DB			
ca		Admin			
fw01		Transit			
		DMZ			
		BL			
		Admin			
		DB			
		Management			
prxy01		DMZ			
repo		Admin			

2.4.2.5 Subsystems and Software Components

Table 7 and Table 8 show the subsystems and the software components deployed in the CISE Node (type A-B).

Table 7. CISE Node - Subsystems.

Hostname	Software	Version
adm01	Apache ActiveMQ	
	Apache2 HTTP server	
	HSQL Database Engine	
	Jboss Liferay	
	Wildfly	
	MariaDB database server	
	Nagios Core	
	Nagios NRPE	
bl01	Apache ActiveMQ	
	Wildfly	
	Nagios NRPE	
	Docker	
dbms01	PostgreSQL database server	

Hostname	Software	Version
	Docker	
	Nagios NRPE	
ca		
	Wildfly	
	MariaDB database server	
	bind9	
	Nagios NRPE	
prxy01	Afterlogic WebMail on Apache2 HTTP server	
	Apache2 HTTP server	
	Apache Artemis	
	Consul	
	bind9	
	ProFTPD	
	dovecot	
	OpenLDAP server (slapd)	
	Nagios NRPE	
	Apache Openmeetings	
	postfix	
	Squid HTTP Proxy	

Table 8. CISE Node - specific software components.

Hostname	Software component	Version
bl01	eucise-core-services	
	eucise-com-gateway-service-app	
adm01	eucise-portal-01.01	
	eucise-theme	
	audit-service-accounting-web	
	audit-service-accounting	
	audit-service-logging-web	
	audit-service-logging	
	audit-service-monitoring-ear	
	audit-service-monitoring	

2.4.2.6 High-Availability Option

The high-availability option includes the following changes in the configuration A-B minimum:

- Use of VMWare High-Availability.
- Duplication of resources: VMs, internal and external firewalls.
- Use of the VRRP protocol.
- Use of load balancers: ZEVENET.
- Use of Gluster (https://www.gluster.org/).
- Use of DRBD, Corosync and Pacemaker.
- Changes in the deployment and configuration process.

3 Networking

The network between CISE Nodes is a point-to-point network with no central component for management nor monitoring the communication. A virtual private network (VPN) is established between nodes using Internet, as transport means, and the IPSEC protocol for securing the communications, as shown in Figure 18.

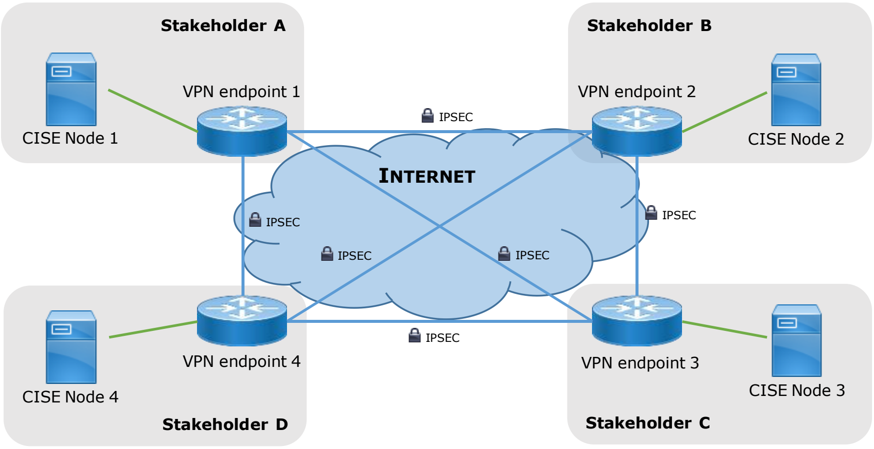


Figure 18. The network between CISE Nodes (VPN).

Only the CISE Nodes can be connected to the secure network. The node owner is responsible for the secure connection between the CISE Node and the VPN endpoint. Each stakeholder relies on their own network/Internet provider to connect the CISE Node with the other nodes.

VPN endpoints correspond with the external firewall depicted in Figure 16 (extfw01-nodeRC). However, the configuration may be different due to specific requirements from each stakeholder.

The IPSEC configuration between VPN endpoints is specific for each connection. Node administrators (or network administrators) must agree the IPSEC parameters applied in each connection. For the guidance of the stakeholders, the following IPSEC parameters were recommended:

Table 9. Recommended IPSEC parameters for the VPN.

Parameter Description	Preferred	Allowed

The stakeholders are responsible for the security of the network between CISE Nodes and the adaptors/ legacy systems connected to them (Figure 19).

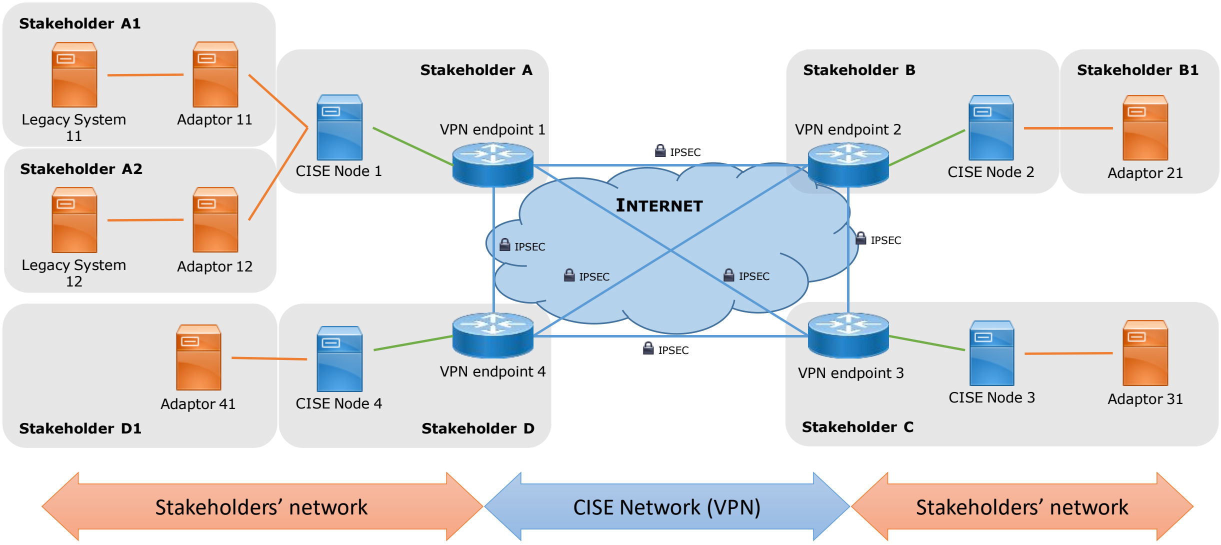


Figure 19. The network between CISE Nodes, including adaptors and legacy systems.

The current network configuration can be used to exchange unclassified information, which includes sensitive information, such as personal information or commercial-sensitive.

4 The pre-operational CISE network

The pre-operational CISE network is the unclassified secure network designed and developed during the EUCISE 2020 project (http://www.eucise2020.eu).

One of the main objectives of the CISE Transitional Phase is to maintain and consolidate the pre-operational CISE network and interoperability building blocks.

The status of the CISE Network at the end of the validation period of the EUCISE 2020 project (March 2019) is the following:

- 10 CISE nodes offering information services
  - From 9 EEA Member States: Finland, Germany, Norway, Portugal, Bulgaria, France, Greece, Italy and Spain
  - Using 19 adaptors for 17 legacy systems
- 2 CISE nodes without legacy systems
  - Dissemination Hub, hosted by ASI, for demo purposes
  - Research Hub, hosted by JRC, as connection hub to other research projects.

Figure 20 depicts a representation of the pre-operational CISE network.

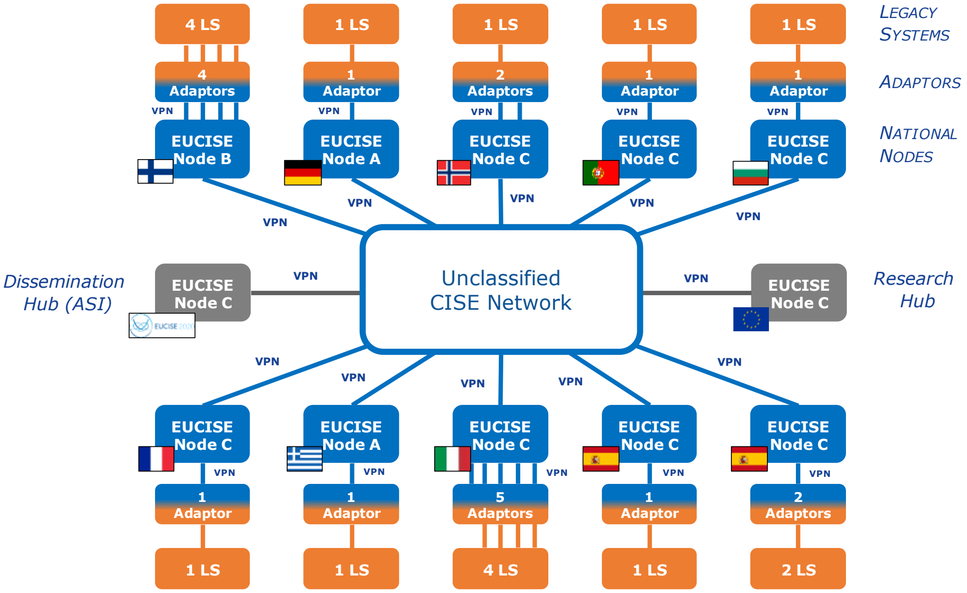


Figure 20. Pre-operational CISE Network (March 2019).

5 Documentation

For additional information, the following documents from the EUCISE2020 project are available:

On the configuration of the CISE Node:

1) M0203EUCIS1SVD01 – Software Version Document (SVD), version 01.00, 07/05/2019
2) M16081.02.1122TM – User manual of EUCISE2020 system, version 02.00, 15/03/2019
3) M16081.02.1123TM – Manual of EUCISE2020 Administrator, version 02.00, 15/03/2019

On the adaptor:

4) M16081.02.1072TR – Interface control document for national adaptors, version 01.00, 27/11/2017

On the pre-operational CISE Network

5) M16081.02.1031TR D3.1-UNCLAS Testbed deployed

Note: The CISE Support Team cannot distribute these resources until the IPR transfer between EUCISE 2020 and the European Commission is signed.