CISE Architecture

Version 3.1
Date: 18/02/2025

Project funded
by the European Union

Document History

Version	Date	Changes
1.0	20/05/2019	Initial version
2.0	04/03/2022	Removed information from CISE Node v1. Added information on the CISE Node v2. Added links to additional information.
3.0	11/01/2024	Last updates from the CISE Network. Added information on the CISE Node v2.
3.1	18/02/2025	Update of section 3. Documentation

Table of Contents

List of Tables

List of Figures

List of Abbreviations

CISE	Common Information Sharing Environment for the Maritime Domain
EEA	European Economic Area
EU	European Union
ICT	Information and Communication Technologies
VPN	Virtual Private Network

1. The CISE Architecture

The CISE Architecture describes how the Maritime CISE[1] should work and how information is exchanged in the Maritime CISE.

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 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.

This document summarises the main aspects of the CISE Architecture. The objective is to help the reader understand how CISE works and how CISE could help their organisation to exchange information with others through the CISE interoperability solution.

1.1 Key Principles

The Maritime CISE is driven by the five key principles:

- 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 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.

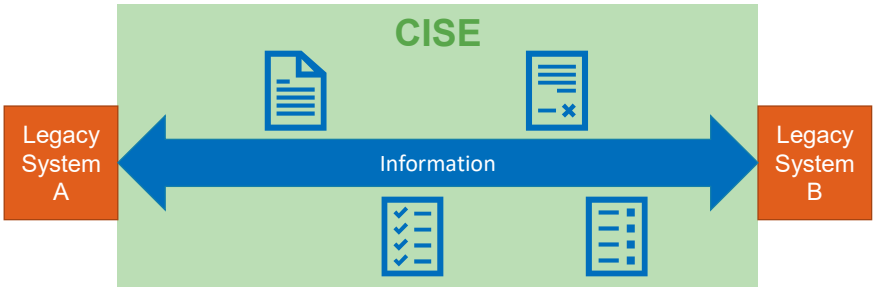


Figure 1. Point-to-point information exchange in CISE.

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 needs.

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] http://emsa.europa.eu/cise.html
https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en

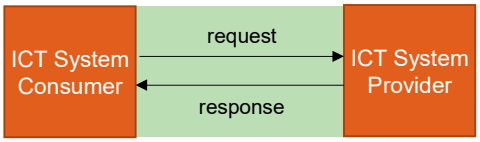


Figure 2. Pull communication pattern.

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.

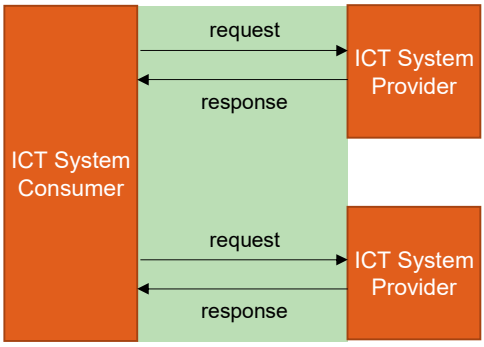


Figure 3. Pull Unknown communication pattern.

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).

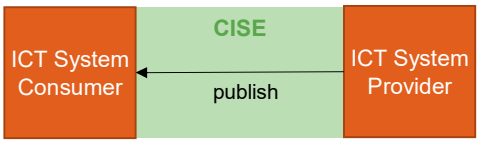


Figure 4. Push communication pattern.

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.)

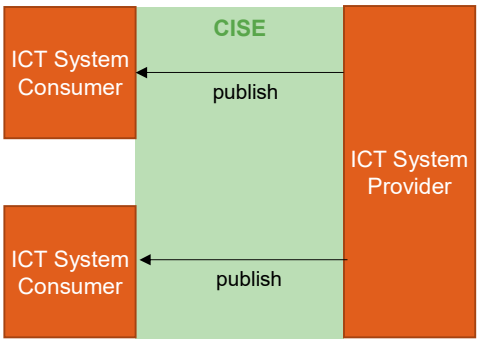


Figure 5. Push Unknown communication pattern.

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.

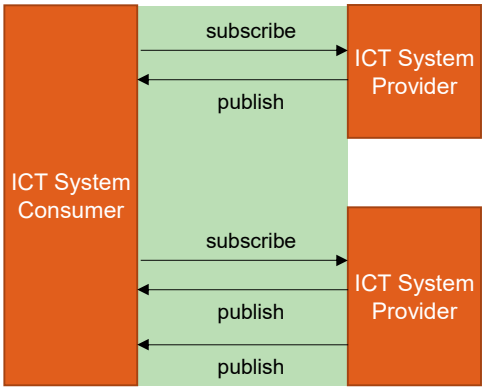


Figure 6. Publish/subscribe communication pattern.

1.3 Building blocks and responsibilities

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

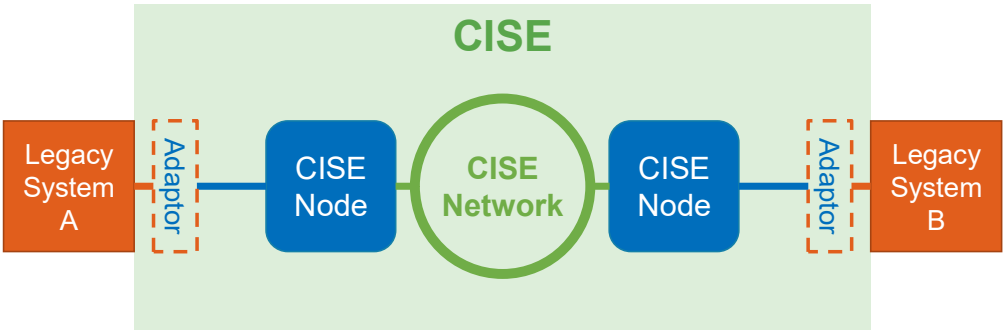


Figure 7. Main building blocks of the CISE Architecture.

- **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**[2]: 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 Using the Building Blocks

In the CISE Architecture, stakeholders 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 in a Member State. This section describes different possible combinations of building blocks.

1.4.1 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.

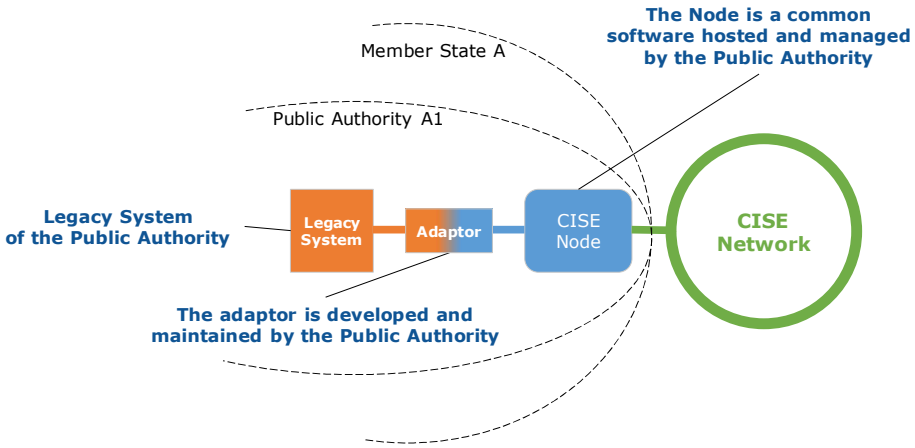


Figure 8. Legacy system directly connected to the CISE network.

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.

[2] Adaptors/legacy systems are called 'participants' in the CISE Node.

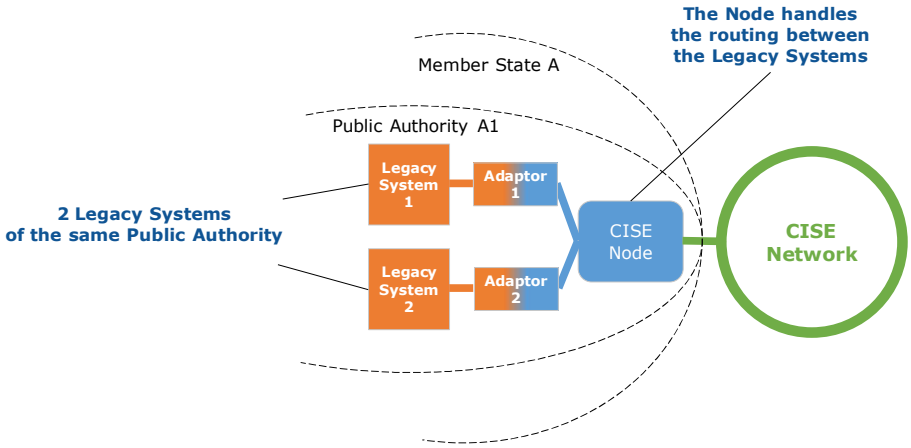


Figure 9. Two legacy systems directly connected to the CISE network using a single node.

1.4.2 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, one of the stakeholders will manage the CISE node.

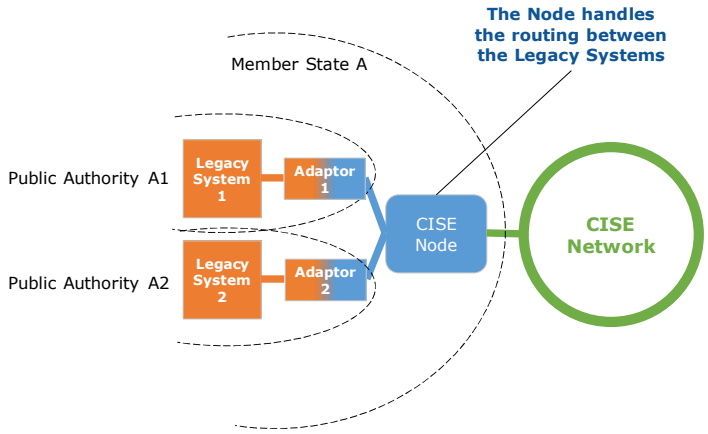


Figure 10. Legacy systems using a shared CISE node to connect to the CISE Network.

1.4.3 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. One of the stakeholders will manage the CISE Node.

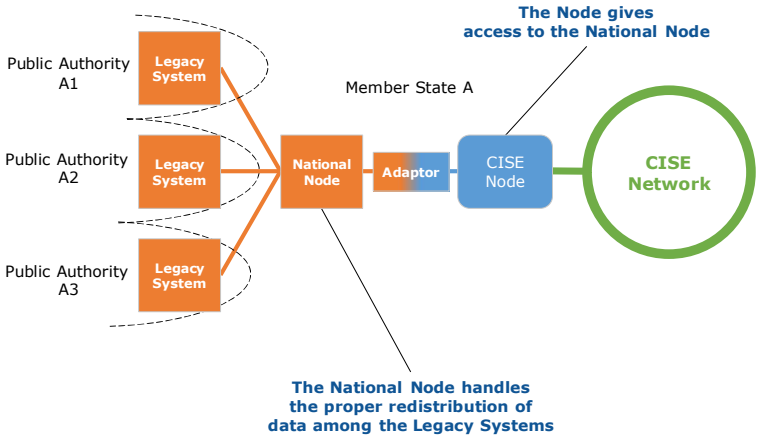


Figure 11. Legacy systems connected through a National Node.

1.5 Interoperability Standards

Interoperability in CISE is based on two standards, which are implemented in the building blocks:

- The CISE Data model: common language for information exchange.
- The CISE Service model: communication protocol for CISE.

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.

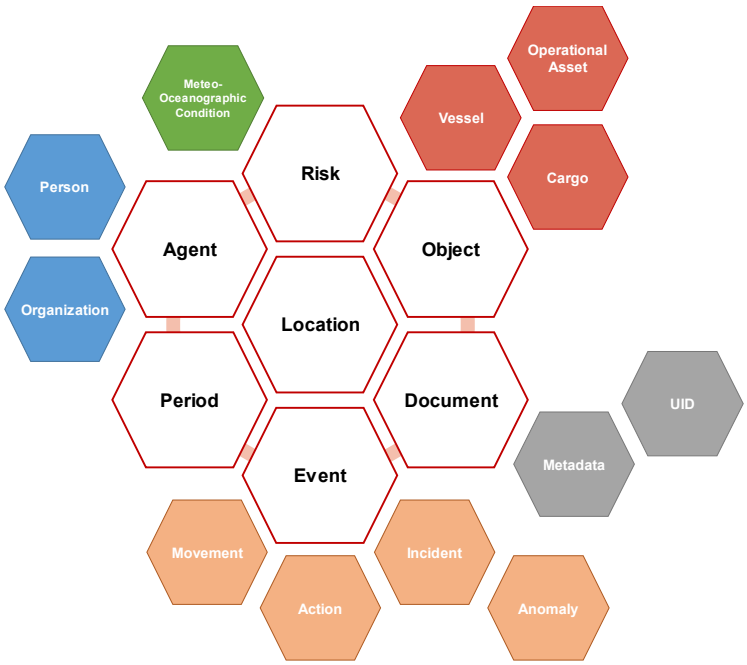


Figure 12. Representation of the main and auxiliary entities in the CISE Data model.

More information on the CISE Data Model: https://emsa.europa.eu/cise-documentation/cise-data-model-1.5.3/

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.

Figure 13. Four corners in the communication protocol.

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)*

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.).

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.

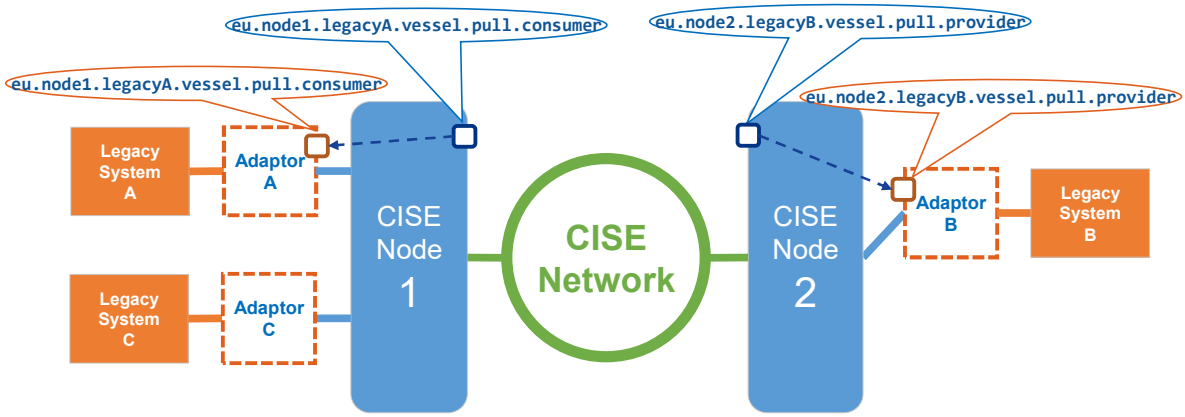
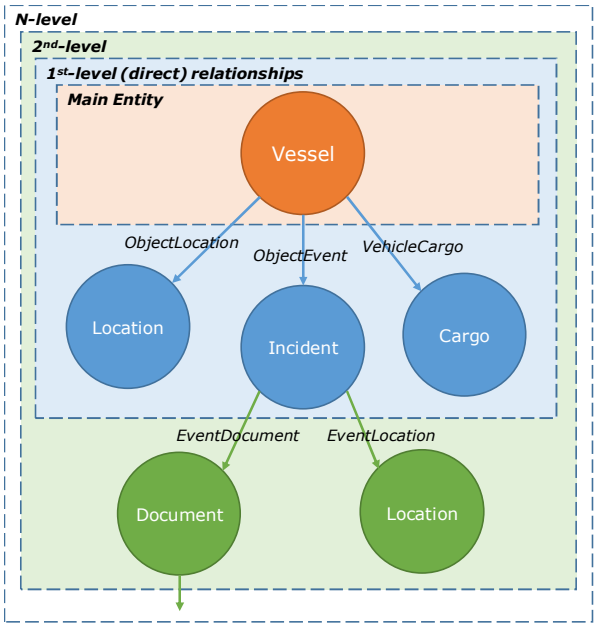


Figure 14. Information services, initial scenario.

Information services are defined by the following metadata:

Element	Description
Service ID	Unique identifier of a service in CISE following an agreed scheme (URN). Participants will define the service IDs within the namespace assigned to them.

Element	Description
	eu.nodeA.systemA.vessel.pull.consumer.vesselService123 Top-level domain Node ID Participant ID Service type, operation, role Service name
Service Type	Main data entity exchanged using this service. For instance, a service of type VesselService exchanges vessel data. Annex 1 contains a list of the possible service types in the CISE service model. 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 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: 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	Metadata describing the capabilities of the service:

Element	Description
Capabilities	• subscription capabilities; • maximum number of concurrent connections; • maximum delay time to receive a reply.
Service Provider	ID of the Legacy System (participant) that offered the service, e.g., eu.nodeA.systemA

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

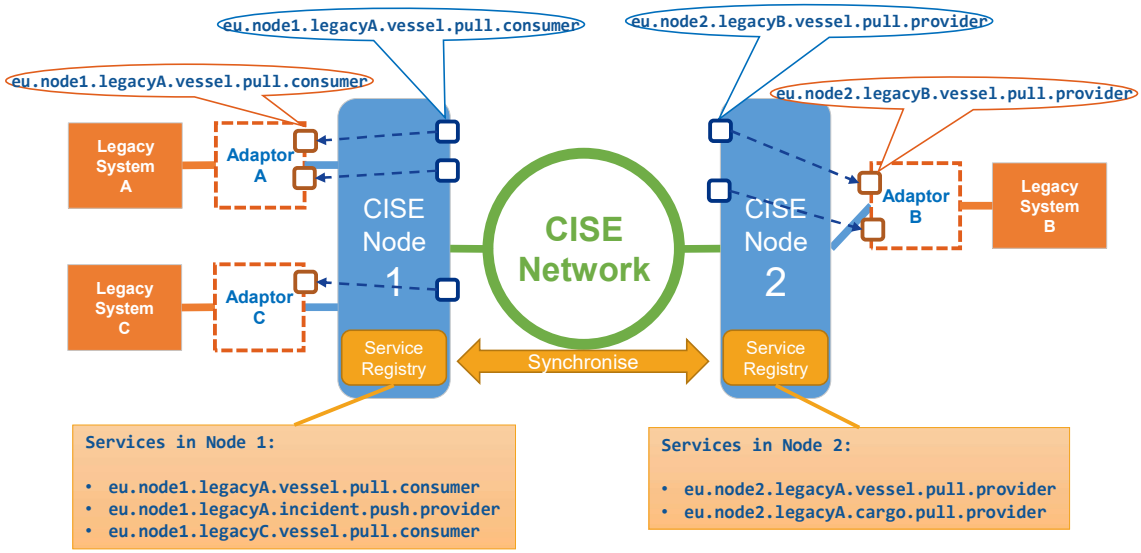


Figure 15. Service metadata in the CISE Network.

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), e.g., fd5b2bb2-8095-4acf-b6cb-3dd78ba8a572
  - CorrelationID: Needed to reply to another message. Message ID (UUID) of the message that started the communication flow.
  - ContextID: ID (UUID) of the communication, which links 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 it is encoded in the type of the CISE message.

Message Type	Actions
PullRequest	• Request information. • Subscribe/unsubscribe from a service. • Retrieve the service subscribers.
PullResponse	• Provide information, after request. • Communicate any error in the request.
Push	• Provide information, with no previous request.

Acknowledgement	• Confirms message reception.
	• Communicates errors in the protocol.
	• Two types of acknowledgements:
	  ○ Synchronous, from the local node (corner 2) indicates that the message is valid and can be processed.
	  ○ Asynchronous, indicates that the message was delivered to corner 4. from the "other" node (corner 3), to indicate that the message was delivered to Corner 4.

Feedback	• 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

The payload includes the data exchanged, formatted using the CISE Data Model, and additional meta-information on the payload: data sensitivity, etc. Payloads may 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.
- Message, describing the messages required to invoke an information service, an/or receive information.
- Participant, describing the metadata related to legacy systems/adaptors.

More information on the data structures can be found at: http://emsa.europa.eu/cise-documentation/

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.

Table 2. Message types by communication pattern.

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

More information on the message flow can be found at: http://emsa.europa.eu/cise-documentation/

1.5.2.5 Access rights

Information providers can define an access rights matrix on each CISE information service (provider). The Access Rights Matrix is an ordered set of access control rules, each of which specify:

- A target group: a group of consumer services (i.e., the target group) allowed to receive the information.
- The access permissions: what is made available and restrictions.
    - Information (i.e., main entity's attributes, relationships) will be made available.
    - The period when the information will be available.
    - Geographic constraints for the information exchanged (limitation by bounding box).

If no access rule is defined, the access to the information is denied by default.

Access control rules are defined, managed and enforced in the CISE Node. However, the information providers could enforce additional checks in the adaptors and/or legacy systems.

2. The CISE Node

The CISE node is the building block that 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.

The first version of the CISE Node was developed in the context of the EUCISE 2020 pre-operational validation FP7 project (2015-2019). The version 2 of the CISE Node was released in October 2021, updating the architecture and the technology stack. The CISE Node version 2.0 is compatible with existing adaptors but it cannot communicate with instances of the CISE nodes version 1.

2.1 Functionalities

The functionalities implemented in the CISE Node are grouped into the following service categories:

- **Core and Common Services**: capabilities to 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
    - Application security services
        - Identification/Authentication of users
        - Management of access rights to the information
    - Capabilities to exchange information using the CISE interoperability standards.
    - Auditing services: capabilities to understand how information is exchanged in the CISE Network and to monitor the performance of the Network. Three categories: logging, monitoring, and accounting.
- **Collaborative services**: capabilities to enable the communication and collaboration among the operators: Instant messaging, e-mail, video and voice conference, whiteboard, file transfer, shared document repository and shared calendar.
    - These capabilities are not included yet in the CISE Node version 2.
- **Data Streaming Services**: capabilities to stream data in well-known formats across the CISE Network, in which the use of the CISE interoperability standards is not possible.
- **Management Services:** capabilities to control and facilitate the use of the CISE Node.
    - Administration console: the Administration Console enables authenticated users to manage the CISE Node.
    - APIs: Remote management of the CISE Node, e.g., from the adaptors or legacy systems.

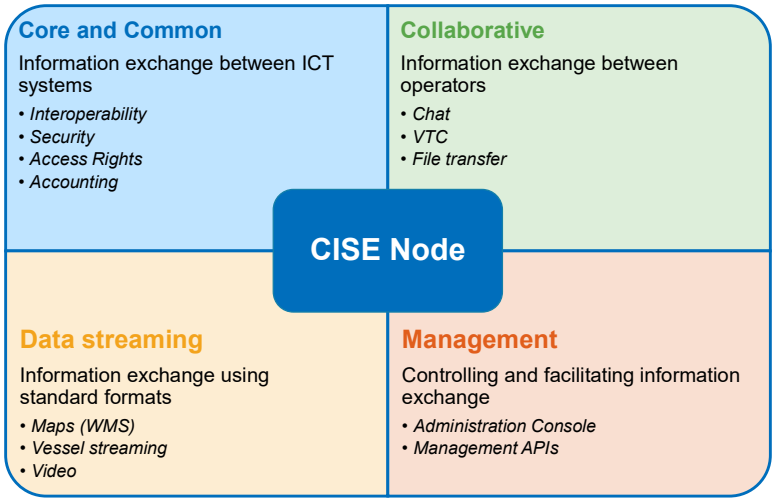


Figure 16. Functionalities covered in the CISE Node.

2.2 Node Architecture

The functionalities of the CISE Node are implemented in several software components and subsystems, which are deployed across a set of virtual machines in the same virtual network. The node was designed to be resilient and scalable at a low cost for the stakeholders.

2.2.1 Logical Architecture

The CISE Node version 2 was designed with a microservice architecture. The functionalities of the CISE Node were split in small components with a single purposed, decoupled at network level.

2.2.2 Technical Specifications

The technical specifications (hardware, virtual infrastructure, and network) of the CISE Node version 2 are available in the Welcome Package to all the CISE stakeholders. Please check Section 4 how to request access.

2.2.3 External Interfaces of the CISE Node

The CISE Node exposes different external interfaces to the other corners of the communication.

For more information, please see Section 4.

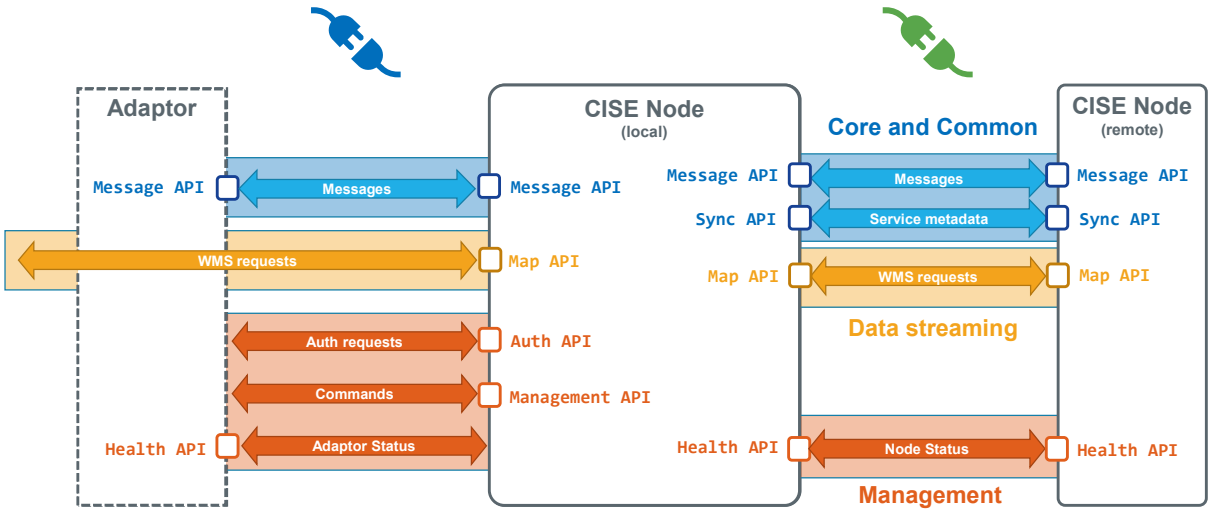


Figure 17. External interfaces of the CISE Node.

2.3 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.

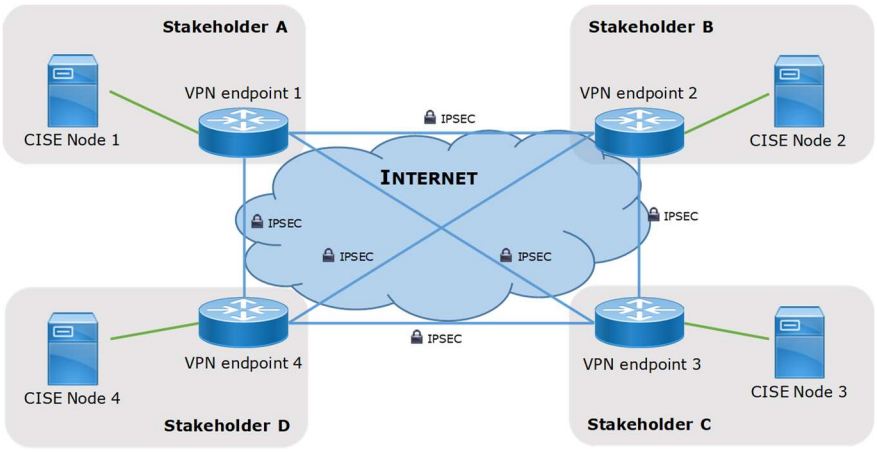


Figure 18. The network between CISE Nodes (VPN).

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, as well as, between the CISE Node and the adaptors/legacy systems.

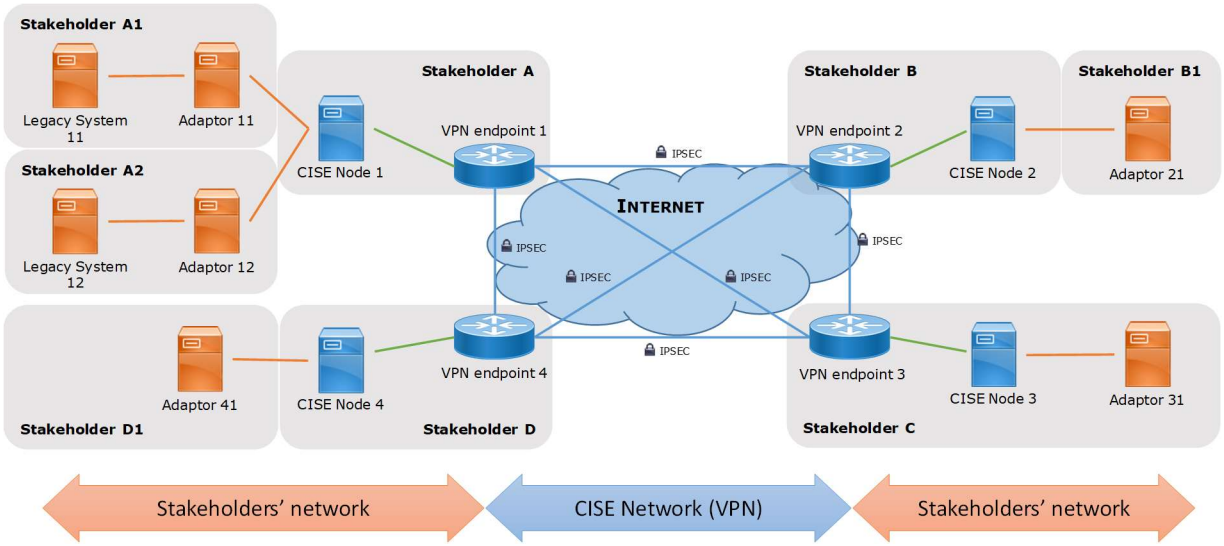


Figure 19. The network between CISE Nodes, including adaptors and legacy systems.

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

The requirements to establish a network for classified information will be analysed during the Transitional Phase.

3. Documentation

Additional information is available on the CISE web site (https://emsa.europa.eu/cise) and in the Welcome Package for CISE Stakeholders (CISE collaborative site, MS Teams).

The CISE stakeholders can ask for support on the available documentation at any time by sending an email to mss@emsa.europa.eu

Appendix A Service types in the CISE Service Model

ServiceType	Description
ActionService	Services of this type exchange information of type Action as main entity.
AgentService	Services of this type exchange information of type Agent as main entity.
AircraftService	Services of this type exchange information of type Aircraft as main entity.
AnomalyService	Services of this type exchange information of type Anomaly as main entity.
CargoDocumentService	Services of this type exchange information of type CargoDocument as main entity.
CargoService	Services of this type exchange information of type Cargo as main entity.
CertificateDocumentService	Services of this type exchange information of type CertificateDocument as main entity.
CrisisIncidentService	Services of this type exchange information of type CrisisIncident as main entity.
DocumentService	Services of this type exchange information of type Document as main entity.
EventDocumentService	Services of this type exchange information of type EventDocument as main entity.
IncidentService	Services of this type exchange information of type Incident as main entity.
IrregularMigrationIncident Service	Services of this type exchange information of type IrregularMigrationIncident as main entity.
LandVehicleService	Services of this type exchange information of type LandVehicle as main entity.
LawInfringementIncident Service	Services of this type exchange information of type LawInfringementIncident as main entity.
LocationDocumentService	Services of this type exchange information of type LocationDocument as main entity.
LocationService	Services of this type exchange information of type Location as main entity.
MaritimeSafetyIncidentService	Services of this type exchange information of type MaritimeSafetyIncident as main entity.
MeteoOceanographicCondition Service	Services of this type exchange information of type MeteoOceanographicCondition as main entity.
MovementService	Services of this type exchange information of type Movement as main entity.
OperationalAssetService	Services of this type exchange information of type OperationalAsset as main entity.
OrganizationDocumentService	Services of this type exchange information of type OrganizationDocument as main entity.
OrganizationService	Services of this type exchange information of type Organization as main entity.
PersonDocumentService	Services of this type exchange information of type PersonDocument as main entity.
PersonService	Services of this type exchange information of type Person as main entity.
RiskDocumentService	Services of this type exchange information of type RiskDocument as main entity.
RiskService	Services of this type exchange information of type Risk as main entity.
VesselDocumentService	Services of this type exchange information of type VesselDocument as main entity.
VesselService	Services of this type exchange information of type Vessel as main entity.

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu