ETSI GS CDM 002 V1.1.1 (2021-03)

Common information sharing environment service and Data Model (CDM); System Requirements definition

Disclaimer

The present document has been produced and approved by the european Common information sharing environment service and Data Model 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
DGS/CDM-002

Keywords
data sharing, maritime, safety, service

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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 a Communication "Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain (CISE)", promoting to integrate maritime surveillance activities of all public maritime sectors across Europe (Figure 1).

Figure 1: Schematic diagram of the CISE vision

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, Defence, as well as the economic interests of the EU, so as to facilitate sound decision making.

The added value of integrating maritime surveillance is to enhance the present sectoral maritime awareness pictures of the sectoral user communities, with additional relevant cross-sectoral and cross-border surveillance data on a responsibility to share basis. Such enhanced pictures increase Member States authorities' efficiency and improve cost effectiveness.

Thus, the decentralized information exchange system is directed to interlink all relevant User Communities, taking into account existing sectoral information exchange networks and planned systems, and allowing for the improvement and development of both the existing sectoral systems, and the overarching CISE network architecture (Figure 2).

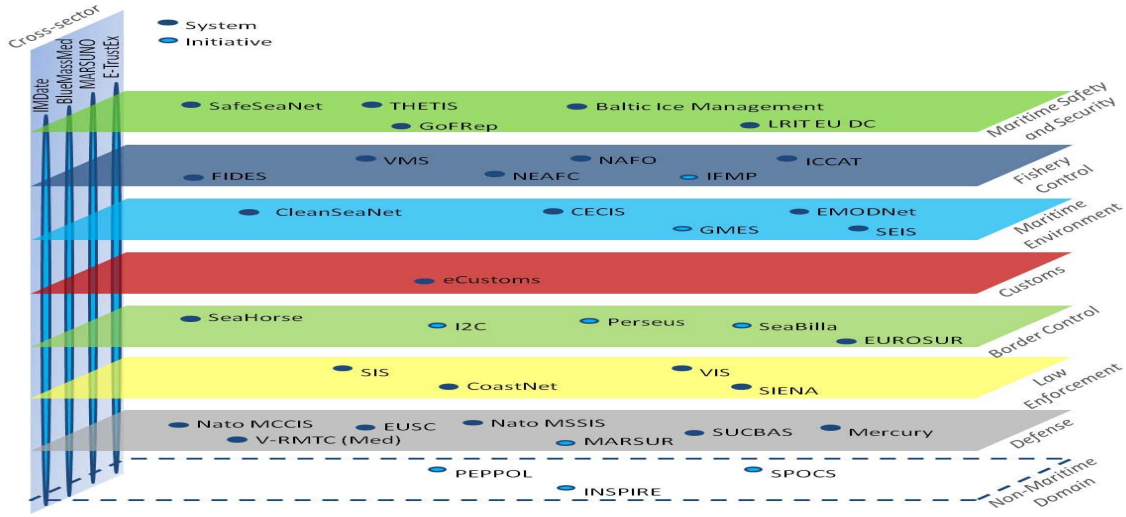

Figure 2: Existing sectoral information systems

To achieve the goals of the CISE vision, a series of EU sponsored projects, building up one on another, further investigated and developed the CISE vision, starting with the elaboration of the so-called CISE principles, which were defined as follows [i.2]:

- *"CISE must allow the interlinking of any public authority in the European Union (EU) or European Economic Area (EEA) involved in maritime surveillance."*
- *"CISE must increase maritime awareness based on the "responsibility-to-share" principle."*
- *"CISE must support a decentralized approach at EU-level."*
- *"CISE must provide interoperability between civilian and military information systems."*
- *"CISE must be compatible and provide interoperability between information systems at the European, national, sectoral and regional levels."*
- *"CISE must support the reuse of existing tools, technologies and systems."*
- *"CISE must provide for seamless and secure exchange of any type of information relevant to maritime surveillance."*
- *"CISE must support the change of services by information provider (orchestration)."*
- *"CISE subscribers and stakeholders should be entitled to obtain information only if they also contribute in a way commensurate with their capabilities."*

The CISE roadmap process that started with the definition of the CISE principles is shown in Figure 3.

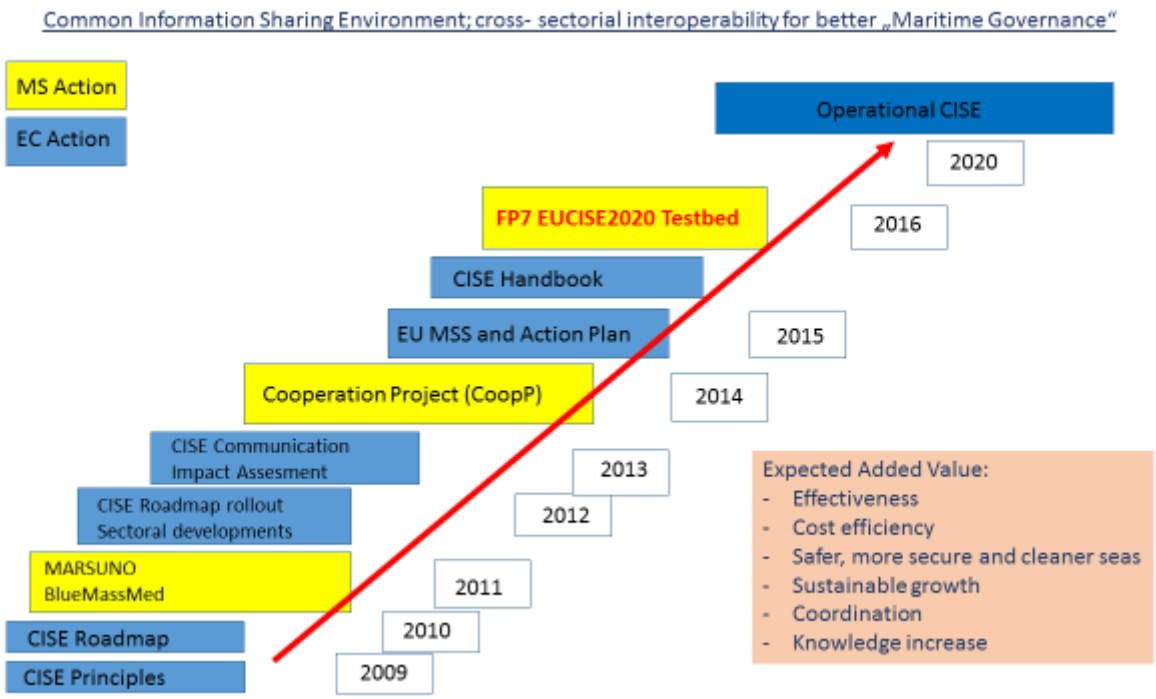

Figure 3: CISE Roadmap

During the roadmap process, a range of 82 use cases was defined representing the entire range of activities of the 7 maritime sectors and their related Coast Guard activity. Out of this range of 82 use cases, 9 use cases were identified as most characteristic and comprehensive, covering the most relevant activities of all sectors. These use cases were to form the operational basis for the further and more detailed investigation of CISE cross- sectoral and cross border information exchange.

The pre-operational validation project **"European test bed for the maritime Common Information Sharing Environment in the 2020 perspective"**, in short **"EU CISE2020"**, based on the 9 use cases selected, defined the requirements and developed the common architecture of the CISE information exchange network. Consequently, a total of 12 so-called "CISE Nodes" were built, integrated and successfully tested in 9 European countries, connecting a total of 20 sectoral legacy systems of various nature (Figure 4).

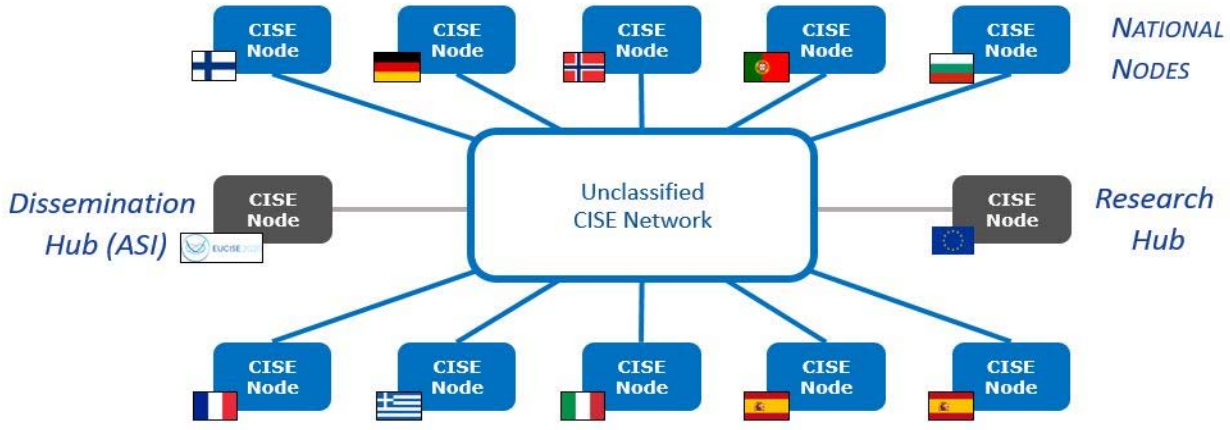

Figure 4: Diagram of the EUCISE 2020 testbed set- up

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 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.

1 Scope

The present document defines the System Requirements for the European Common information sharing environment service and Data Model (CDM). The requirements are based on the operational use cases described in ETSI GR CDM 001 [i.1].

The present document addresses requirements in the following broad areas:

- Architecture.
- Infrastructure (Core Services):
  - Network and Communication Security.
  - Message Routing.
  - Identification, Authentication and Authorization.
  - Service Discovery.
  - Auditing (Logging, Monitoring and Accounting).
  - Administration User Interface.
  - Collaboration Tools.
- Interface (Common Services):
  - Information Exchange.
  - Message Structure.
  - Data Model.
- Performance.

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.

Not applicable.

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.

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 not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR CDM 001 (V1.1.1): "Common Information Sharing Environment Service and Data Model (CDM); Use Cases definition".

[i.2] CISE Architecture Visions Document V3.0 06/11/2013.

NOTE: Available at https://webgate.ec.europa.eu/maritimeforum/en/node/4039.

[i.3] Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU). Official Journal of the European Union, L274, 3-52.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR CDM 001 [i.1] and the following apply:

activity: One of the following activities performed by a sector:

- for the maritime safety, security and prevention of pollution sector:
  - vessel traffic management;
  - vessel traffic safety;
  - monitoring of security of ships;
  - search and rescue;
  - support of response and enforcement operations (anti-piracy, SAR, salvage);
- for the fisheries control sector:
  - early warning of illegal fisheries or fish landings;
  - monitoring of compliance with regulations on fisheries;
  - support of response and enforcement operations;
- for the marine pollution preparedness and response sector:
  - monitoring of compliance with regulations;
  - early warning of environmental accidents and incidents;
  - support of pollution response operations;

- for the customs sector:
  - monitoring of compliance with customs regulation on import, export and movement of goods;
  - support of enforcement operations;
- for the border control sector:
  - monitoring of compliance with regulations on immigration and border control crossings;
  - support of enforcement operations;
- for the general law enforcement sector:
  - monitoring of compliance with applicable legislation in sea areas where police competence is required;
  - support to enforcement and response operations;
- for the defence sector:
  - monitoring in support of defence tasks such as national sovereignty at sea;
  - combatting terrorism and other hostile activities outside the EU;
  - other CSDP tasks as defined in Articles 42 and 43 of TEU.

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

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

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

cross-sector: (exchange of information) between two or more Sectors

EUCISE 2020: FP7 pre-operation validation project on CISE

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

NOTE 2: More information on the project can be found at http://www.eucise2020.eu/.

EU RESTRICTED: classified information covered by the definition of EU security classification levels [i.3]

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.

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

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

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

node: set of software components providing CISE infrastructure and access point to CISE network

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

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

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

provider: participant providing Service over CISE network

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

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

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

sea basin: sea area

NOTE: The following sea areas are identified:

- Atlantic.
- Baltic Sea.
- North Sea.
- Mediterranean.
- Black Sea.
- Outermost Regions.
- Arctic Ocean.

sector: user community involved in maritime surveillance

NOTE: The existing 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.

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

UNCLASSIFIED: information not covered by the definition of EU security classification levels [i.3]

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:

AUI	Administration User Interface
CISE	Common Information Sharing Environment
CSDP	Common Security and Defence Policy
CT	Collaboration Tools
DM	Data Model
EEA	European Economic Area
EFTA	European Free Trade Association
EU	European Union
FP7	Seventh Framework Programme of the European Union
GR	Group Report
IAA	Identification, Authentication and Authorization
IE	Information Exchange
IT	Information Technology
JRC	Joint Research Center
LMA	Logging, Monitoring and Accounting
MR	Message Routing
MS	Message Structure
NC	Network Communication
SAR	Search And Rescue
SD	Service Discovery
SOA	Service Oriented Architecture
TCP/IP	Transmission Control Protocol/Internet Protocol
TEU	Treaty on European Union

4 Overview

Most of the system requirements in the present document are originally inherited from the EUCISE 2020 project. However, not all the operational and technical requirements identified during the procurement phase of the EUCISE 2020 project have been included. The requirements have also been edited and modified so that they do not appear in their original form in the present document.

Requirements have been divided into functional and performance requirements. Functional requirements have been further divided into architecture, infrastructure and interface requirements.

5 Functional requirements

5.1 Architecture

CISE aims to provide direct information exchange capability between European Public Authorities across borders and sectors by enabling direct machine-to-machine and human-to-human connections via a common network. In some cases there is need to exchange also classified information up to EU RESTRICTED level.

CISE infrastructure involves high amount of hardware components, communication lines and software modules installed, maintained and controlled by multiple actors. Thus, the probability of an occasional failure occurring in some part of the network is quite high. However, CISE is intended to support 24/7 activities.

The following requirements aim to secure that CISE supports information exchange between relevant legacy systems, is resilient to occasional modifications and failures in some part of the network and is able to support also the exchange of classified information:

[Fun-Arc-01] CISE architecture shall support Services versioning that allows two or more versions of the same Service to coexist.

[Fun-Arc-02] CISE architecture shall be designed to be resilient to the unavailability of network or Services provided by a Participant. It shall recover automatically when these Services or the network are available again.

[Fun-Arc-03] CISE architecture should provide mechanisms for handling classified information up to EU RESTRICTED level.

[Fun-Arc-04] CISE architecture shall be designed in such a way that the failure of any component does not prevent any other non-dependent components from functioning.

[Fun-Arc-05] CISE architecture shall provide TCP/IP connection to exchange information among Legacy Systems.

5.2 Infrastructure (Core Services)

5.2.1 General

CISE infrastructure provides the environment for information exchange. It handles the identification, authentication and authorization of participants, facilitates service discovery and exchange and stores information on network activities and performance. Clause 5.2 documents requirements related to the CISE infrastructure and its functions.

5.2.2 Network and Communication Security

Information exchanged via CISE network is intended to support Public Authorities carrying out their Activities. These include baseline operations, targeted operations and response operations as described in ETSI GR CDM 001 [i.1]. Some of the information exchanged can be classified, sensitive or contain personal data. It is important that Participants are able to trust that all the information is exchanged timely, unchanged and protected from eavesdropping.

The following requirements intend to secure the integrity and security of data exchanged via CISE network:

[Fun-NC-01] CISE shall prevent unauthorized access to the CISE network.

[Fun-NC-02] CISE shall guarantee integrity and origin of any data stored or transported in CISE network.

[Fun-NC-03] At transport layer, CISE shall ensure information exchange over a secure channel.

[Fun-NC-04] All Messages exchanged through CISE shall be asynchronous to decouple the CISE infrastructure from Legacy Systems.

[Fun-NC-05] CISE shall implement a mechanism for prioritizing the Messages.

[Fun-NC-06] Any Messages transported shall not block the delivery of any other Messages.

[Fun-NC-07] CISE shall implement a retry mechanism including a number of retransmissions and delay between consecutive retransmissions to ensure the proper delivery of Messages in case of an error. The mechanism shall be configurable.

5.2.3 Message Routing (Network Service)

ETSI GR CDM 001 [i.1] describes information exchange needs between CISE Participants in different operational scenarios. Depending on the nature of the event and actors involved, information exchange could be initiated either by the Provider or the Consumer. Starting point for the information exchange could be, for example, one of the following:

- Participant needs information and knows who can provide it.
- Participant needs information but does not know who can provide it.
- Participant has information and knows who needs it.
- Participant has information but does not know who needs it.
- Participant needs information on regular basis and knows who can provide it.

The following requirements describe the identified message patterns needed and the general messaging rules:

[Fun-MR-01] CISE shall support the PULL pattern. In this pattern, a Participant (Consumer) requests information from a known list of other Participants (Providers). The CISE shall deliver the request to the list of Providers and transfer the response in an asynchronous way.

[Fun-MR-02] CISE shall support the PUSH pattern. In this pattern, a Participant (Provider) notifies information to a known list of other Participants (Consumers). The CISE shall deliver the notification.

[Fun-MR-03] CISE shall support the PULL Unknown pattern. In this pattern, a Participant (Consumer) request information from unknown list of other Participants (Providers). CISE shall deliver the request to a list of Providers selected automatically based on the Service profile provided by the Consumer (see clause 5.2.5).

[Fun-MR-04] Upon the PULL Unknown Request from a Consumer, CISE shall answer with the number and identifier of Providers which are able to provide information.

[Fun-MR-05] CISE shall support the PUSH Unknown pattern. In this pattern, a Participant (Provider) notifies information to unknown list of other Participants (Consumers). CISE shall deliver the information to a list of Consumers selected based on their pre-announced interest and the access rights set by the Provider. The Consumers should announce their interest towards Services by using Service profile parameters (see clause 5.2.5).

[Fun-MR-06] Upon the PUSH Unknown notification from a Provider, the CISE shall answer with the number and identifier of Consumers.

[Fun-MR-07] CISE shall support PUBLISH/SUBSCRIBE pattern. In this pattern, a Participant (Consumer) can subscribe notifications from another Participant (Provider). CISE shall deliver notifications from the Provider automatically to a list of Participants who have subscribed for the information and who has right to access the information. It shall be possible to subscribe or unsubscribe notifications at any time.

[Fun-MR-08] In case of multicast communication, CISE shall not aggregate the different answers.

[Fun-MR-09] For each CISE Message, the CISE shall detect and ignore duplicated Messages.

5.2.4 Identification, Authentication and Authorization

CISE network connects Public Authorities belonging to different Sectors, carrying out different Activities and handling data that can contain confidential, sensitive and/or personal data. Although it is technically possible to exchange all kinds of data directly between any of the CISE Participants, the data exchange needs to respect information exchange agreements. Thus it is vitally important that all Participants are uniquely identified and authenticated. In some cases, the Provider is able to freely distribute the data to any other Participant, but in some other cases, the Provider needs to limit access to the data.

The following requirements intend to provide reliable identification of Participants and enable flexible access control:

[Fun-IAA-01] The Node Administrator only shall be allowed to add, update and delete CISE Participants connected to that Node.

[Fun-IAA-02] Each Participant shall be identified by an unique identifier and described by a Participant profile including at least the following attributes:

- Name and description of the Legacy System.
- Nationality.
- Participant's Sectors.
- Participant's Activities.
- Sea Basin.
- Security level (i.e. EU RESTRICTED, UNCLASSIFIED).

- Point of contact information.
- List of provided Services.

[Fun-IAA-03] CISE shall allow discovery of the CISE Participants with at least the following criteria:

- Sector.
- Activity.
- Nationality.
- Sea Basin.

[Fun-IAA-04] A CISE Participant with UNCLASSIFIED security level shall not be able to discover a CISE Participant with EU RESTRICTED security level.

[Fun-IAA-05] CISE architecture shall provide authentication of CISE Participants. The evidences of the authentication shall be logged.

[Fun-IAA-06] The authentication profiles of each CISE Participant shall be federated with the chain of trust.

[Fun-IAA-07] CISE shall ensure that Services are accessible only to those authorized to have access.

[Fun-IAA-08] The CISE shall provide a mechanism to grant or deny access to Services and to define access rights to the information elements provided by the Service.

[Fun-IAA-09] The access right rules shall be configurable. Only the Node Configuration Manager role should be allowed to configure and modify the access right rules.

[Fun-IAA-10] CISE shall check the permission to deliver information to a CISE Participant following the access right rules and based on:

- Participant Sectors.
- Participant nationality.
- Participant Activities.
- Sea Basins.

5.2.5 Service Discovery (Service Manager)

CISE will increase maritime situational awareness based on the "responsibility-to-share" principle. Following this principle, it is expected that all Public Authorities connected to CISE network will actively make data from their Legacy Systems available via CISE in machine-readable format. With large amount of Services available, there is need to have a mechanism that enables to find the data of interest in the most efficient way.

The following requirements aim to make sure that Participants are able to automatically discover and request relevant Services among all the Services available in the CISE network:

[Fun-SD-01] Each CISE Service shall be defined by a Service profile with at least the following information:

- Service type (describing the entities exchanged).
- Service operation (describing the message pattern e.g. PULL, PUSH, PUBLISH/SUBSCRIBE).
- Sea Basin.
- Service status.
- Service Provider (identifying the CISE Participant providing the Service).
- Service capabilities (describing the Service performance parameters).

[Fun-SD-02] The status of a CISE service during its lifetime shall be one of the following:

- DRAFT: When a new Service is created, it shall be in the DRAFT status for initial testing purposes. The Service shall be available only to the CISE Participant providing the Service.
- ONLINE: When the Service is published to the CISE Network and available to the CISE Participants that have access to it according to the access right rules it shall be in the ONLINE status.
- MAINTENANCE: When the Service is under maintenance and not available to CISE Participants it shall be in the MAINTENANCE status. The Service or the Service profile shall be modified only in MAINTENANCE status.
- DEPRECATED: When two or more versions of the same Service are available from the same Provider, the older version(s) of the Service shall be in the DEPRECATED status.
- OFFLINE: When the Service is not available any more, it shall be in the OFFLINE status.

[Fun-SD-03] CISE Services shall allow to declare at least the following Service performance parameters:

- Response time.
- Maximum number of result.
- Maximum number of request per time unit.
- Refresh rate.

[Fun-SD-04] CISE shall allow the discovery of Services exposed with at least the following criteria:

- Participant Sector.
- Participant Activity.
- Nationality.
- Sea Basin.
- Service type.
- Service capabilities.
- Service operation.

5.2.6 Auditing (Logging, Monitoring and Accounting)

Since information that is exchanged between Participants in CISE network could contain confidential, sensitive and/or personal data, it is important to keep track on and store all information exchange actions between partners.

In addition, the efficient maintenance of CISE network requires frequent monitoring and logging of performance and status of its hardware and software components.

Stored data enables the creation of usage analytic reports to support various verification and validation procedures.

The following requirements have been identified:

[Fun-LMA-01] CISE shall store Service request and responses performed by any CISE Participant (accounting data). The stored data shall include metadata that specifies what data elements have been requested and provided but the actual content of data elements shall not be stored. Stored data shall enable to produce reports regarding the frequency of Service usage.

[Fun-LMA-02] CISE shall trace each personal data exchanged and shall enable to produce dedicated reports of such data exchanged.

[Fun-LMA-03] At least the following shall be stored related to each exchanged Message:

- Identity of CISE Consumer.

- Identity of CISE Provider.
- Activity of the Consumer.
- Service type and information elements exchanged.

[Fun-LMA-04] CISE shall store the log messages and errors created by system software components (logging data).

[Fun-LMA-05] Log messages created by system software components shall be classified as:

- FATAL, severe errors that cause premature termination.
- ERROR, runtime errors or unexpected conditions.
- WARN, runtimes situation that are undesirable or unexpected, but not necessarily wrong.
- INFO, interesting runtime events (start-up/shutdown).
- DEBUG, detailed information on the flow through the system.

[Fun-LMA-06] CISE shall test and store periodically the status and availability of Node components and network resources (monitoring data).

[Fun-LMA-07] All stored accounting, logging and monitoring data shall be accessible in textual format and located in the same CISE Node where it was created.

[Fun-LMA-08] The system shall keep configurable retention periods for all auditing data. The retention periods shall be defined by Node Administrator role. Different retention periods may be defined for different Service types (accounting data).

5.2.7 Administration User Interface

CISE network needs to allow adding, updating and removing Participants, Services and the related access rights. There might be organisational changes among Public Authorities and new systems providing new services are deployed. Agreements related to data exchange between Participants might also change.

The following requirements have been identified:

[Fun-AUI-01] Node shall provide a password protected user interface for Users acting as a Node Administrator and Node Configuration Manager.

[Fun-AUI-02] The user interface shall allow Users to perform the functions listed in the Table 1 below according to their roles.

Table 1

Function	Node Administrator	Node Configuration Manager
Manage Participants of their Node (add, update, delete).	Shall be allowed	Shall not be allowed
Manage Services of their Node (add, update, delete).	May be allowed	Shall be allowed
Manage access right rules of their Node (add, update, delete).	May be allowed	Shall be allowed
Configure auditing functions of their Node (see clause 5.2.6).	Shall be allowed	Shall not be allowed
Monitor the system resources of their Node using indicators and statistical charts.	Shall be allowed	Shall not be allowed
View and export data and reports stored by auditing functions of their Node described in clause 5.2.6.	Shall be allowed	Shall be allowed
Search Participants of all the Nodes connected to the CISE network.	Shall be allowed	Shall not be allowed
Search Services of all the Nodes connected to the CISE network.	May be allowed	Shall be allowed

5.2.8 Collaboration Tools

In addition to the machine-to-machine data exchange, there is also need for CISE to provide tools for cross-border and cross-sector human-to-human interaction. As stated in ETSI GR CDM 001 [i.1], collaboration tools are especially useful when planning targeted operations or coordinating response operations.

The following requirements have been identified:

[Fun-CT-01] The collaboration tools shall support CISE Users in sharing knowledge, experience and expertise, providing near real time and multimedia applications for:

- E-mail.
- Instant messaging.
- Video and voice conferencing.
- White board.
- File transfer.
- Shared document repository.
- Shared calendar.

5.3 Interface (Common Services)

5.3.1 General

Public Authorities' Legacy systems handle and store data in various formats. However, inside the CISE network, there is only one common CISE "language". Participants use CISE language when interfacing the CISE network for discovering, requesting or providing data. CISE interface specifies the format of data requests and responses, message structure in general and the data model used. Clause 5.3 documents requirements related to the CISE interface exposed to CISE Participants.

5.3.2 Information Exchange

The use cases identified in ETSI GR CDM 001 [i.1] show the need to filter the information exchanged between Participants. Targeted data requests and checking that messages are correctly formatted before they are transmitted help to avoid overloading the CISE network and the connected Legacy systems.

The following requirements have been identified:

[Fun-IE-01] CISE shall support requests based on:

- Time period.
- Geographical area.
- "Query by example" based on information elements exchanged.

[Fun-IE-02] CISE shall support requests with a validity period. The response may be disregarded after the validity period.

[Fun-IE-03] CISE shall check that all Messages are properly formatted.

[Fun-IE-04] CISE shall provide a mechanism to ensure the data quality of the information exchanged. This mechanism shall allow:

- Provider to modify or delete information already sent.
- Consumer to provide feedback to the Provider on the information received.

5.3.3 Message Structure

CISE supports a number of messaging patterns (see clause 5.2.3) which enable Participants to discover, request and provide data related to the different use cases described in ETSI GR CDM 001 [i.1]. The messaging patterns are realized by the exchange of structured Messages between Participants in a controlled manner.

In addition to the data that Participants agree to exchange using the common data model (see clause 5.3.4), the Messages need to contain also additional information related to originator, recipient and properties of the exchanged data.

The following requirements have been identified:

[Fun-MS-01] Each PULL request Message shall allow to specify at least the following:

- Time limit after which the response may not be considered by the requesting system.
- Activity for which the requested data is used.
- Identity of the requesting Participant.

[Fun-MS-02] Each PULL response, PUSH and PUBLISH Message shall allow to specify at least the following:

- The retention period of the information provided.
- If the Message contains personal information.
- Data classification.

[Fun-MS-03] Each SUBSCRIPTION request Message shall allow to specify at least the following:

- Time period of the subscription.
- Activity for which the subscribed data is used.
- Identity of the subscribing Participant.

[Fun-MS-04] For each Message sent that contains personal data, the retention period shall be provided.

[Fun-MS-05] Participant shall receive an acknowledgement whenever a Message is delivered or in case of an error. In case of a request Message, the status of the request shall be returned including information about the success of the communication process, data formatting and access rights permission.

5.3.4 Data Model

CISE is expected to interlink a wide variety of existing information systems, which handle and store data using many different standardized or proprietary formats. A CISE data model defines common data format and semantics for all the data exchanged. The use of a common data model enables to preserve the meaning of the exchanged data unchanged and also automatically check the consistency of the exchanged data.

The following requirements have been identified:

[Fun-DM-01] CISE shall ensure the exchange of information related to vessels, operational assets and cargo.

[Fun-DM-02] CISE shall ensure the exchange of risk information.

[Fun-DM-03] CISE shall ensure the exchange of information related to persons and organizations.

[Fun-DM-04] CISE shall ensure the exchange of information related to events such as movements, actions, incidents and anomalies.

[Fun-DM-05] CISE shall ensure the exchange of information related to meteo-oceanographic conditions.

[Fun-DM-06] CISE shall ensure the exchange of information related to locations.

[Fun-DM-07] CISE shall ensure the exchange of documents, such as reports or structured information.

[Fun-DM-08] CISE shall enable the exchange of streamed information.

[Fun-DM-09] CISE shall ensure the exchange of a combination of the different information listed in requirements [Fun-DM-01] to [Fun-DM-08] and their relationship to describe a complete maritime situation.

6 Performance requirements

It is estimated that there are around 400 Public Authorities in Europe that are somehow involved in maritime surveillance [i.2] and CISE needs to be able to connect all of them to the same network.

In some cases, authorities inside the same Member State want to use a joint access point (Node) to connect to CISE. Each connected Public Authority might be able to provide several different Services to CISE network.

Maritime surveillance information ranges from short vessel position reports to satellite images [i.1]. CISE needs to be able to support the exchange of all relevant surveillance information.

The following requirements have been identified:

[Per-Req-01] CISE architecture shall support at least 400 Participants.

[Per-Req-02] CISE Node shall be scalable providing access point to CISE network from one up to at least 20 Participants.

[Per-Req-03] CISE shall support at least 240 Services per Participant.

[Per-Req-04] There shall be at least one User account for collaboration tools per each CISE Participant.

[Per-Req-05] CISE shall be able to transport and process Messages with the size up to at least 100 Megabytes.

Annex A (informative): Bibliography

- EUCISE 2020 project, D4.1: "Needs Analysis".
- EUCISE 2020 project, D4.3: "Technical Specification".
- JRC Technical Report: "The Entity Service Model for CISE" V1.53, 28/02/2017.

History

Document history		
V1.1.1	March 2021	Publication