ETSI GS CDM 002 V2.1.1 (2023-02)

GROUP SPECIFICATION

Common information sharing environment service and Data Model (CDM); System Requirements definition; Release 2

Disclaimer

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

Reference

RGS/CDM-008

Keywords

data sharing, maritime, requirements, safety,
service

ETSI

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

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

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

Important notice

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

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

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

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

In October 2009 the European Commission adopted a Communication "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain", promoting to integrate maritime surveillance activities of all public maritime sectors across Europe [i.2]. This Communication introduced the first general guiding principles of the Common Information Sharing Environment (CISE) and initiated the CISE development process (Figure 1).

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

The following year, in October 2010, European Commission adopted a new CISE related Communication "Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain", which provided the plan for the first concrete actions towards building the CISE [i.3].

The Communication noted that 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 would increase Member States authorities' efficiency and improve cost effectiveness. It was further noted that 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.

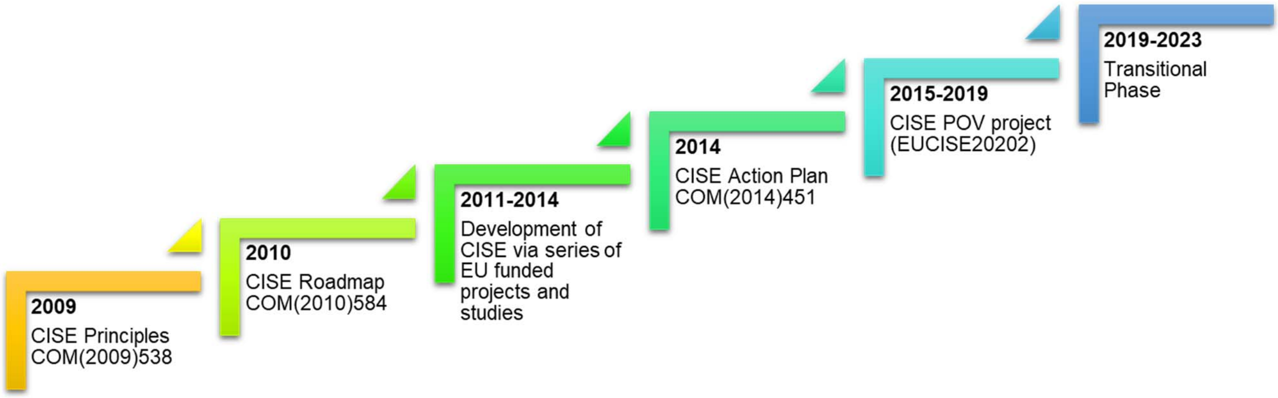

2009
CISE Principles COM(2009)538
2010
CISE Roadmap COM(2010)584
2011-2014
Development of CISE via series of EU funded projects and studies
2014
CISE Action Plan COM(2014)451
2015-2019
CISE POV project (EUCISE20202)
2019-2023
Transitional Phase

Figure 1: CISE development process

During the following years, from 2011 to 2014, a series of EU sponsored projects and studies, building up one on another and supported by JRC and the Member States Technical Advisory Group (TAG), investigated and developed the legal, organizational, semantical and technical interoperability of CISE. The CISE principles were further elaborated [i.4], and number of use cases, covering the most relevant activities of all sectors were identified. Based on these use cases, the first versions of the technical interoperability tools (e.g. data model and communication patterns) were developed.

In July 2014, the European Commission adopted a Communication "Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain", which reported the development already made related to the development of CISE and introduced the planned further activities, including the funding of a large scale CISE Pre-Operational Validation (POV) project [i.5].

The POV project "European test bed for the maritime Common Information Sharing Environment in the 2020 perspective", in short "EUCISE 2020", was launched in 2015. It defined the technical requirements, developed the common architecture and established a CISE information exchange network testbed. 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 2).

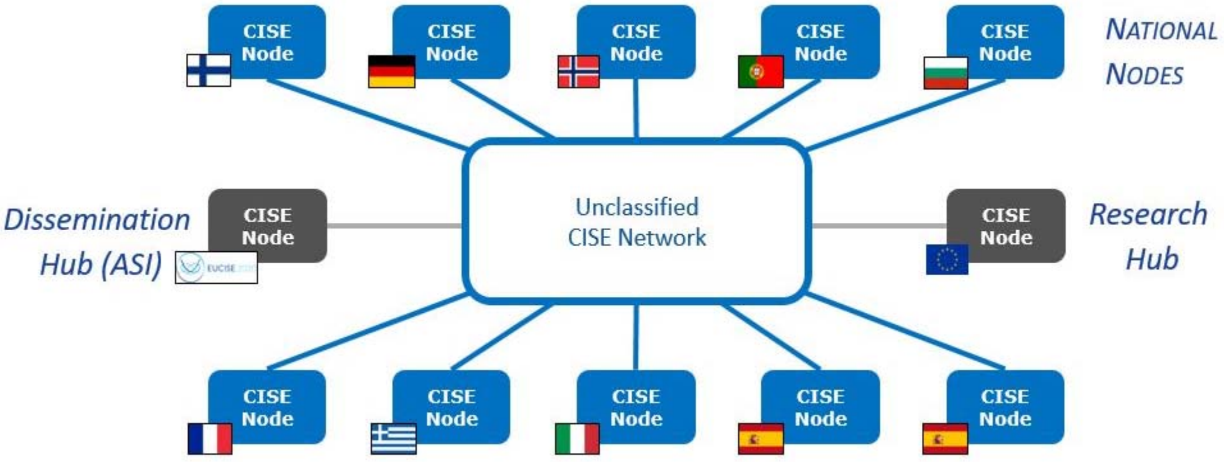
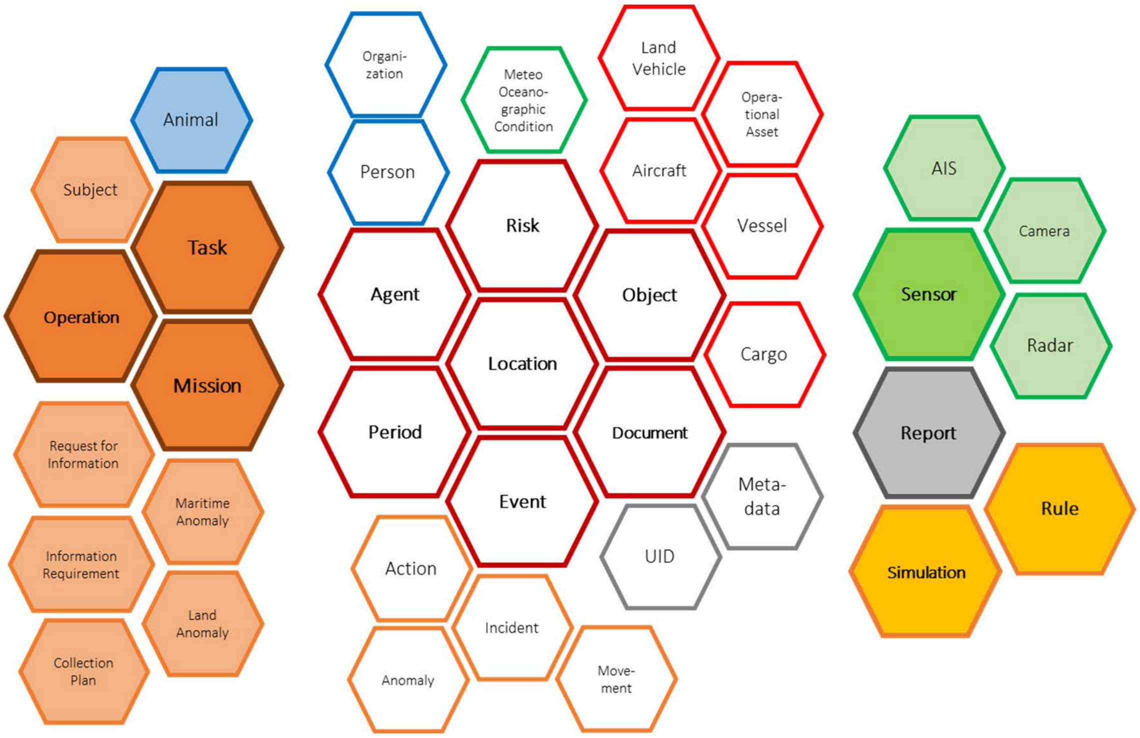


Figure 2: EUCISE 2020 testbed set- up

Following the EUCISE 2020 project, in April 2019, the European Commission started the CISE Transitional Phase. The transitional phase is coordinated by the European Maritime Safety Agency (EMSA) and it will carry out the full implementation of CISE and its transition into operational system by 2023.

Hybrid and complementary cross-sectoral and cross-border information exchange requires a common "data language" within the common network architecture as well as a common set of IT- services to handle the data transfer. The technical standardization proposal for CISE implementation was therefore initiated by EUCISE 2020 project and directed towards a standardization process within the framework of a professional European standardization environment in order to elaborate universal and sustainable technical specifications for the implementation and development of CISE, as well as offering a technical solution for other, similar information exchange regimes. ISG CDM was established in 2019 to carry out the technical standardization of CISE.

The ANDROMEDA project, funded under Horizon2020 in 2019-2021, reused the results from the EUCISE 2020 project and demonstrated that the solution may be adopted for information exchange also in other domains in addition to the maritime domain. ANDROMEDA designed and developed a secure, effective common situational awareness and information exchange system integrated within CISE. The project successfully tested the enhanced CISE Data model (Figure 3), with specific extensions for the exchange of information in the domain of Land Border Surveillance. Based on the results of the ANDROMEDA project, the ISG CDM therefore decided to extend the scope of standardization to the land border surveillance domain.



NOTE: The hexagons in the center of the figure portray the core and auxiliary entities of the CISE Data Model developed by EUCISE 2020 project. The hexagons in the right and left side of the figure (filled with blue, orange, green, grey and yellow colour) portray the extensions introduced by ANDROMEDA project.

Figure 3: Enhanced CISE Data Model

The requirements in the present document respect the operational and technical requirements defined during the CISE development process (Figure 1) and the general principles of CISE as originally defined in [i.2], [i.4] and later elaborated in the most recent version of the CISE Architecture [i.6] as follows:

- CISE connects public authorities in the EU and EEA responsible for maritime surveillance: civil and military, regional/sectorial organizations and EU agencies.
- CISE connects existing maritime surveillance ICT systems. However, CISE is not a new surveillance system, nor a new screen in the surveillance centers.
- CISE promotes a sector-neutral solution: all sectors and systems are important.

- CISE follows a decentralized approach: point-to-point exchange of information.
- Information exchange is voluntary, i.e. not enforced by legislation.

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:
  - Network and communication security.
  - Communication patterns.
  - Identification, authentication and authorization.
  - Information services.
  - Auditing.
- Protocol for Information Exchange:
  - Information exchange.
  - 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 (V2.1.1): "Common Information Sharing Environment Service and Data Model (CDM); Use Cases definition; Release 2".

[i.2] Commission Communication COM(2009) 538 final: "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain".

[i.3] Commission Communication COM(2010) 584 final: "on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain".

[i.4] CISE Architecture Visions Document V3.0 06/11/2013.

[i.5] Commission Communication COM(2014) 451 final: "Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain".

[i.6] CISE Architecture Version 2.0, 04/03/2022.

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 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 where police competence is required;
  - support to enforcement and response operations;
- 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 defence Sector:
  - monitoring in support of defence tasks such as national sovereignty;
  - combatting terrorism and other hostile activities outside the EU;
  - other CSDP tasks as defined in Articles 42 and 43 of TEU.

In addition, the following applies to maritime surveillance 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).

agent: person, animal or organization involved as an actor or a target in the various Events related to maritime and land border surveillance

connected system: ICT system belonging to a participating Public Authority or Sector designed to perform specific tasks and exposing certain functionalities through interface

NOTE 1: A connected system can be an existing system or a future system maintained by a Public Authority or Sector and acts as the originator and/or destination of Messages exchanged in CISE network.

NOTE 2: In the present document, a connected system includes the required functionality needed to connect to the CISE Node. The functionality can be provided by a separate software module between the connected ICT system and the Node or it can be integral to the connected ICT system.

NOTE 3: Connected Systems are often referred to as "legacy systems".

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

cross-border: between EU or EFTA countries

cross-sector: between two or more Sectors

EUCISE 2020: FP7 pre-operation validation project on CISE

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

event: movement, anomaly, incident or action which occur in the maritime or land border domain

information element: entity or attribute used in a data model

NOTE: Entities and attributes are used to model real-world objects and their properties respectively.

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

node: software system providing CISE infrastructure and access point to CISE network

node administrator: person appointed to manage local Connected Systems and local Node software, hardware and network connections

object: physical entity in the maritime or land border domain like vehicle (e.g. vessel, aircraft, land vehicle or operational asset) or cargo

provider: connected system providing Service over CISE network

public authority: any organization or legal entity that has an interest in 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 and land border 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 and/or land border surveillance

NOTE: The existing Sectors are the following:

- customs;
- border control;
- general law enforcement;
- fisheries control;
- pollution preparedness and response, marine, deltaic and river environment;
- defence.

The following Sector only applies to maritime surveillance:

- maritime safety, security and prevention of pollution by ships.

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

3.2 Symbols

Void.

3.3 Abbreviations

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

CISE	Common Information Sharing Environment
CSDP	Common Security and Defence Policy
DM	Data Model
EEA	European Economic Area
EFTA	European Free Trade Association
EMSA	European Maritime Safety Agency
EU	European Union
FP7	Seventh Framework Programme of the European Union
GR	Group Report

IAA	Identification, Authentication and Authorization
ICT	Information and Communications Technology
IE	Information Exchange
IT	Information Technology
JRC	Joint Research Center
LMA	Logging, Monitoring and Accounting
MR	Message Routing
MS	Message Structure
NC	Network Communication
POV	Pre-Operational Validation
SAR	Search And Rescue
SD	Service Discovery
SOA	Service Oriented Architecture
TAG	Member States Technical Advisory Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TEU	Treaty on European Union

4 Overview

Requirements have been divided into functional and performance requirements. Functional requirements are presented in clause 5. Functional requirements have been further divided into architecture, infrastructure and information exchange protocol requirements in corresponding clauses 5.1, 5.2 and 5.3. Performance requirement are presented in clause 6.

Most requirements in the present document are independent of the domain. These are common requirements. However, some requirements apply only to a specified domain (i.e. maritime). These requirements are domain specific extensions of the common requirements.

Common requirements are identified by a combination of abbreviated main clause name (i.e. Fun or Per), two or three letter descriptive code (e.g. related to the sub clause name) and a sequential number (e.g. "Fun-IAA-02" for a Functional requirement on Identification, Authentication and Authorization). In case of domain specific extensions of common requirements, the domain identifier (i.e. Maritime) is added to the end of the requirement identifier (e.g. "Fun-IAA-02-Maritime" for maritime domain specific extension of a common Functional requirement on Identification, Authentication and Authorization).

5 Functional requirements

5.1 Architecture

CISE network aims to provide direct information exchange capability between European Public Authorities across borders and Sectors by enabling direct machine-to-machine connections via a common network. In some cases there is need to exchange also unclassified sensitive information like, for instance, personal data.

CISE network 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 network is intended to support 24/7 activities.

The following requirements aim to secure that the CISE Node supports information exchange between Connected Systems, is resilient to occasional modifications and failures in some part of the network and is able to support also the exchange of sensitive information:

[Fun-Arc-02] A Node shall be resilient to the unavailability of network connection and/or Services provided by Connected Systems. It shall recover automatically when these Services and/or the network connections are available again.

[Fun-Arc-03] A Node shall provide mechanisms for handling unclassified sensitive information.

[Fun-Arc-04] A Node shall be resilient to the failure of any of its components. It shall recover automatically when the component is available again.

[Fun-Arc-05] A Node shall interact with other Nodes and Connected Systems using a network TCP/IP connection.

5.2 Infrastructure

5.2.1 General

The Node provides the infrastructure for information exchange. It handles the identification, authentication and authorization of Connected Systems, facilitates Service discovery and exchange and stores information on network events. Clause 5.2 documents requirements related to the Node 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 sensitive, e.g. contain personal data. It is important that Public Authorities 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] A Node shall prevent unauthorized access to the CISE network.

[Fun-NC-02] A Node shall guarantee integrity and origin of any data that is received, sent or stored.

[Fun-NC-03] A Node shall ensure information exchange over a secure channel with other Nodes and Connected Systems.

[Fun-NC-04] The communication protocol between Nodes and between Nodes and Connected Systems shall be asynchronous.

[Fun-NC-05] A Node shall implement a mechanism to prioritize the exchange of information between Connected Systems.

[Fun-NC-06] A Node shall support concurrent exchanges of information between Connected Systems.

[Fun-NC-07] A Node shall implement a retry mechanism to ensure the delivery of the information to the Connected Systems. The mechanism shall be configurable and allow to define at least a number of retransmissions and the delay between consecutive retransmissions.

5.2.3 Communication patterns

ETSI GR CDM 001 [i.1] describes information exchange needs between Public Authorities 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:

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

The following requirements describe the identified communication patterns:

[Fun-MR-01] A Node shall support the PULL pattern. In this pattern, a Consumer requests information from a known Provider. A Node shall deliver the request to the Provider and transfer the response back to the Consumer in an asynchronous way.

[Fun-MR-02] A Node shall support the PUSH pattern. In this pattern, a Provider notifies information to a known Consumer. A Node shall deliver the notification.

[Fun-MR-03] A Node shall support the PULL Unknown pattern. In this pattern, a Consumer request information from unknown Providers based on their profile. A Node shall discover the available Providers in the network and deliver the request to them automatically.

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

[Fun-MR-05] A Node shall support the PUSH Unknown pattern. In this pattern, a Provider notifies information to unknown Consumers based on their profile. A Node shall discover the Consumers in the network that match the profile, and deliver the information to them.

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

[Fun-MR-07] A Node shall support PUBLISH/SUBSCRIBE pattern. This pattern shall allow a Consumer to subscribe notifications from a Provider. A Node shall deliver notifications from the Provider automatically to Consumers who have subscribed for the information. A Consumer shall be able to subscribe or unsubscribe at any time.

[Fun-MR-08] In Unknown patterns, a Node shall not aggregate the information from Providers.

[Fun-MR-10] In all communication patterns, a Node shall respect the access right rules set by the Provider (see clause 5.2.4).

5.2.4 Identification, Authentication and Authorization

Nodes connect Public Authorities belonging to different Sectors, carrying out different Activities and handling data that can contain sensitive data (e.g. personal data). Nodes enable the exchange of different kinds of data between any of the Connected Systems (point-to-point exchange). However, Connected Systems need to respect the information exchange agreements between Public Authorities. Thus it is vitally important that the Node also facilitates the implementation of these agreements and all Connected Systems are uniquely identified and authenticated when using the Node. The Node needs to provide additional controls to enforce the access rights defined in the information exchange agreements between Public Authorities.

The following common requirements and extended requirements cover the identification of Connected Systems and enable flexible access control. Extended requirements apply when the Node is intended to serve a specified domain (i.e. maritime).

Common requirements:

[Fun-IAA-01] A Node shall manage and control the connection to the local Connected Systems (i.e. Connected Systems connected directly to the Node and not through a remote Node). The access to this configuration shall be restricted only to the Node Administrator.

[Fun-IAA-02] Each Connected System shall be identified by a unique identifier and described by a profile including at least the following information:

- Name and description of the system.
- Country the system belongs to.
- Sectors that use the system.
- Activities that the system is supporting.

- Point of contact (i.e. person or group of persons that can be addressed in case of issue with the Connected System).

[Fun-IAA-03] A Node shall allow discovery of the Connected Systems in the local Node or in the network with at least the following criteria:

- Country the system belongs to.
- Sectors that use the system.
- Activities that the system is supporting.

[Fun-IAA-05] A Node shall authenticate any system directly connected to it, either another Node or the Connected Systems, during their interaction.

[Fun-IAA-07] A Node shall ensure that Services provided by Connected Systems are accessible only to those authorized to have access.

[Fun-IAA-08] A Node shall provide a mechanism to define access rights rules, based on which the Node shall authorize (i.e. grant or deny) access to Services and filter the Information Elements provided by the Service.

[Fun-IAA-09] The access right rules shall be configurable. A Node shall provide a restricted access to configure and modify the access right rules.

[Fun-IAA-10] Access right rules shall include options to authorize Connected Systems at least based on the following metadata:

- Country the system belongs to.
- Sectors that use the system.
- Activities that the system is supporting.

Maritime domain specific extensions:

[Fun-IAA-02-Maritime] In addition to Fun-IAA-02, a Connected System profile shall include the following information:

- Sea Basins that the system covers.

[Fun-IAA-03-Maritime] In addition to Fun-IAA-03, a Node shall allow discovery of Connected Systems with the following criteria:

- Sea Basins that the system covers.

[Fun-IAA-10-Maritime] In addition to Fun-IAA-10, access right rules for authorizing Connected System shall include the following metadata:

- Sea Basins that the system covers.

5.2.5 Information Services

CISE will increase Public Authorities' 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 ICT systems available via the CISE Node in machine-readable format. With large amount of Services available, there is a need to have a mechanism that allows to find the data of interest in the most efficient way.

The following common requirements and extended requirements aim to make sure that Consumers are able to automatically discover and request relevant Services among all the Services available in the CISE network. Extended requirements apply when the Node is intended to serve a specified domain (i.e. maritime).

Common requirements:

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

- Type of the Information Elements provided by the Service.
- Description of the communication pattern supported (i.e. PULL, PUSH, PUBLISH/SUBSCRIBE).
- Identification of the Connected System providing the Service.
- Description of the Service performance parameters.

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

- Average time to provide a response.
- Maximum number of Information Elements the Service is able to provide in a single interaction.
- Maximum number of interactions per time unit the Service is able to process.
- The average information update rate.

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

- Sector that is providing the Service.
- Activity for which the Connected System providing the Service is used.
- Country the Service belongs to.
- Information Elements (i.e. entities and attributes) that the Service provides.
- Communication pattern that the Service supports.

[Fun-SD-05] A Node shall support Services versioning that allows two or more versions of the same Service to coexist.

[Fun-SD-06] A Service shall carry a list of Information Elements of a single type. These Information Elements may be related to other types of Information Elements.

[Fun-SD-07] Information Elements shall be defined following a common data model, thus ensuring semantic interoperability across Connected Systems.

Maritime domain specific extensions:

[Fun-SD-01-Maritime] In addition to Fun-SD-01, Service profile shall have the following information:

- Sea Basin that the Service covers.

[Fun-SD-04-Maritime] In addition to Fun-SD-04, a Node shall allow the discovery of Services exposed with the following criteria:

- Sea Basin that the Service covers.

5.2.6 Auditing

Since information that is exchanged between Connected Systems via CISE network could contain sensitive data (e.g. 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] A Node shall store and manage the events raised during the use of the system. At least the following accounting events shall be stored:

- Information exchange events: Interactions with external systems (i.e. other Nodes or Connected Systems) to exchange information. Only the metadata from the event shall be stored, the actual information shall not be stored.
- Management events: Other than security related changes in the configuration of the Node, changes in the connected Nodes, changes in the Connected Systems, changes in the Services offered by the Node.
- Security events: Changes in the Node users, user interactions, authentication of Connected Systems and other Nodes, changes in the access rights rules, errors when evaluating the access rights.

[Fun-LMA-02] Information exchange events shall register if personal data is exchanged. The Node shall enable to produce reports of such data exchanged.

[Fun-LMA-03] Information exchange events shall register the following information:

- Identity of the Consumer.
- Identity of the Provider.
- Activity of the Consumer.
- Information Elements (i.e. name of entities and attributes) exchanged.

[Fun-LMA-04] A Node shall register and store the errors in the logs of the system, subsystem and software components (raw logging data).

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

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

[Fun-LMA-08] A Node shall enable the configuration of the retention periods for auditing data. A Node shall provide restricted access to configure the retention periods.

[Fun-LMA-09] The Node shall generate reports on the accounting events, logging data and monitoring data.

5.3 Protocol for Information Exchange

5.3.1 General

Clause 5.3 documents requirements of the communication protocol between Connected Systems and the Node.

Connected Systems communicate with the Node using a standard communication protocol. Standard protocol allows to connect to CISE network for discovering, requesting and providing data in an uniform manner.

Public Authorities' ICT systems handle and store data in various formats. However, inside the CISE network, data is exchanged using a common data model. Common data model ensures the semantics of exchanged data, thus securing that Provider and Consumer share the same understanding on the meaning of data. However, when new use cases and application areas for CISE network emerge, there can be need to update and enhance the CISE data model.

5.3.2 Information Exchange

The use cases identified in ETSI GR CDM 001 [i.1] show the need to narrow down the amount of data exchanged by limiting the requested data in time, space and based on the content of Information Elements (i.e. entity and attribute). Targeted data requests help to avoid overloading the CISE network and the Connected Systems.

A Node supports a number of communication patterns (see clause 5.2.3) which enable Connected Systems to request and provide data related to the different use cases described in ETSI GR CDM 001 [i.1]. The communication patterns are realized by the exchange of structured Messages between Consumers and Providers in a controlled manner.

In addition to the data that Consumers and Providers agree to exchange using the common data model, the Messages need to contain also additional information related to the properties and intended use of the exchanged data.

The following requirements have been identified:

[Fun-IE-01] A Node shall support requests limited by:

- Time period.
- Geographical area.
- Information Element properties.

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

[Fun-IE-04] A Node shall provide the following mechanisms to ensure the data quality of the information exchanged:

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

[Fun-IE-05] A Node shall allow the Consumers to indicate:

- The Activity for which the requested information is used for.
- The identity of the Connected System requesting information.
- Time period of the subscription.

[Fun-IE-06] A Node shall allow the Providers to indicate:

- The retention period of the information provided.
- Sensitivity of the information.
- Information containing personal data.

[Fun-IE-07] A retention period shall be provided for information containing personal data.

[Fun-IE-08] A Node shall notify the confirmation of information delivery and/or any error during communication if requested by the Connected System.

[Fun-IE-09] A Node shall support data model versioning.

5.3.3 Data Model

CISE network is expected to interlink a wide variety of existing information systems, which handle and store data using many different standardized or proprietary formats. The 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 basic structure of the CISE data model (Figure 3) has been developed by several consecutive EU funded projects as described in the Introduction part of the present document.

The following requirements related to the data model have been identified:

[Fun-DM-01] Data Model shall enable the exchange of information related to operational assets and other Objects.

[Fun-DM-02] Data Model shall enable the exchange of risk information.

[Fun-DM-03] Data Model shall enable the exchange of information related to Agents.

[Fun-DM-04] Data Model shall enable the exchange of information related to Events.

[Fun-DM-05] Data Model shall enable the exchange of information related to meteo-oceanographic conditions.

[Fun-DM-06] Data Model shall enable the exchange of information related to locations.

[Fun-DM-07] Data Model shall enable the exchange of documents, such as reports or structured information.

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

[Fun-DM-09] Data Model shall enable 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 or land border situation.

6 Performance requirements

It is estimated that there are around 400 Public Authorities in Europe that are somehow involved in maritime surveillance [i.1] and CISE network needs to be able to connect all of them to the same network. When the CISE network is extended to cover additional domains (i.e. land border surveillance) the amount of Public Authorities involved can be even higher.

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

The following requirements have been identified:

[Per-Req-01] A Node shall be able to maintain connection to at least 50 other Nodes.

[Per-Req-02] A Node shall provide access for at least 20 Connected Systems to the CISE network.

[Per-Req-03] A Node shall support at least 240 Services per Connected System.

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.
- CISE Technical specifications and resources maintained by EMSA.
- ADROMEDA project D.3.1 e-CISE Data Model description.

Annex B (informative): Change History

Date	Version	Information about changes
02-2023	2.1.1	The present document has been updated and modified to include support for the land border surveillance domain. Main changes compared to the requirements presented in the ETSI GS CDM 002 V1.1.1 (Common information sharing environment Service and Data Model (CDM); System Requirements definition) are as follows: Clauses 5.2.7 Administration User Interface and 5.2.8 Collaboration Tools and all requirements in those clauses [Fun-AUI-01], [Fun-AUI-02], [Fun-CT-01] deleted. Clause 5.3.3 Message Structure has been deleted and the requirements have been moved to clause 5.3.2 Information Exchange as follows: [Fun-MS-01] and [Fun-MS-03] merged to a new requirement [Fun-IE-05] [Fun-MS-02] transferred to a new requirement [Fun-IE-06] [Fun-MS-04] transferred to a new requirement [Fun-IE-07] [Fun-MS-05] transferred to a new requirement [Fun-IE-08] Clause 5.3.4 Data model renumbered to clause 5.3.3 Data model. Requirement [Fun-Arc-01] from clause 5.1 moved to clause 5.2.5 and renamed to [Fun-SD-05] Requirement [Fun-MR-09] from clause 5.2.3 deleted. Requirement [Fun-IAA-04] from clause 5.2.4 deleted. Requirement [Fun-IAA-06] from clause 5.2.4 deleted. Requirement [Fun-SD-02] from clause 5.2.5 deleted. Requirement [Fun-LMA-05] from clause 5.2.6 deleted. Requirement [Fun-IE-04] from clause 5.3.2 deleted. Requirements [Per-Req-04] and [Per-Req-05] from clause 6 deleted.

History

Document history		
V1.1.1	March 2021	Publication
V2.1.1	February 2023	Publication