ETSI GS CDM 003 V1.1.1 (2021-05)

GROUP SPECIFICATION

Common Information sharing environment service and Data Model (CDM); CDM Architecture

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-003

Keywords
architecture, data models, maritime

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

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

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.

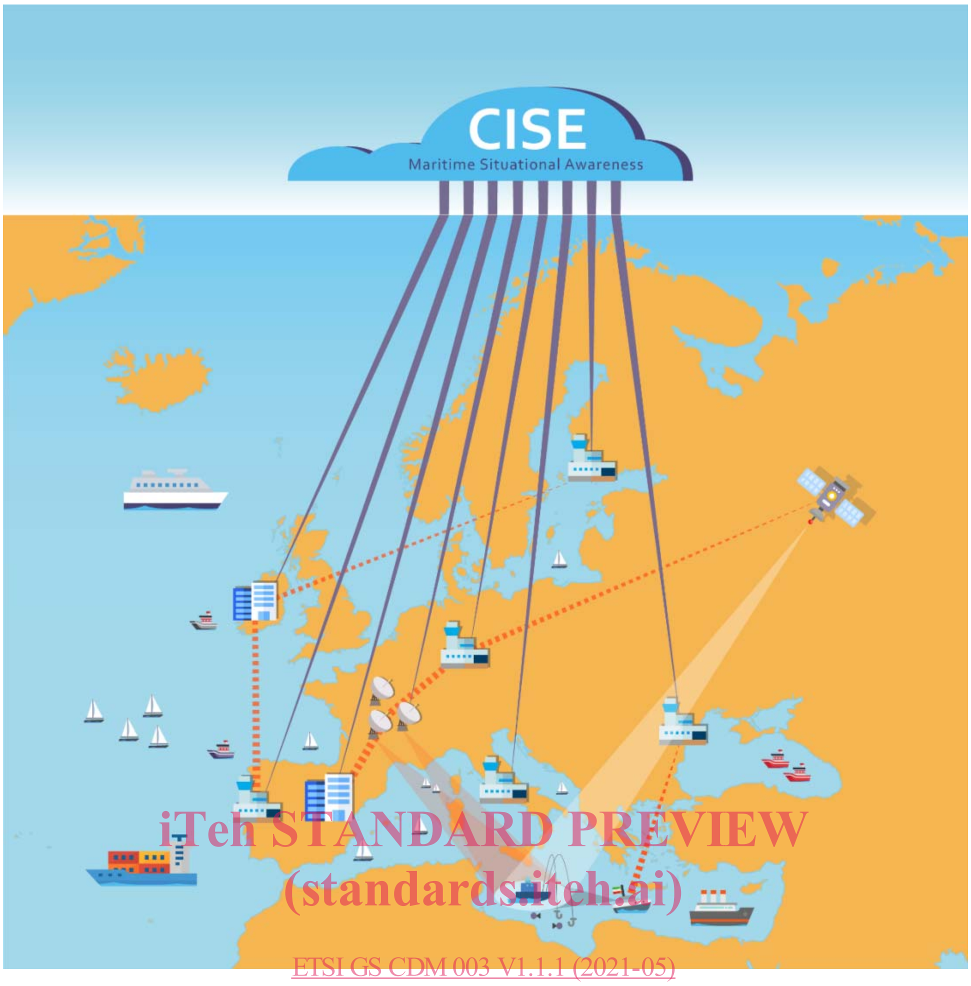

Figure 1: Schematic diagram of the CISE vision

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.

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

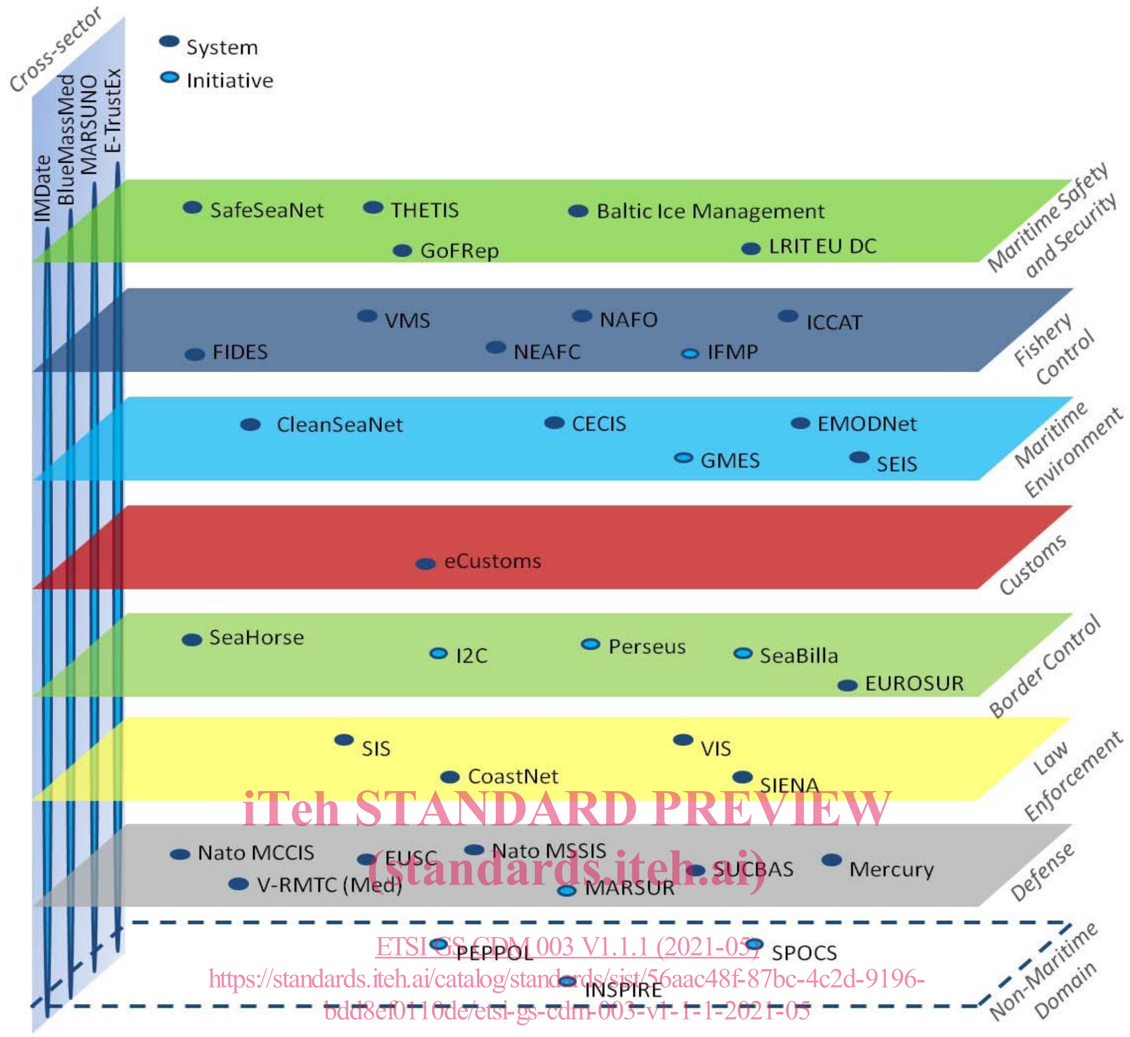

Figure 2: Existing sectoral information systems

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 according to CISE Architecture Visions Document [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 decentralised 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:

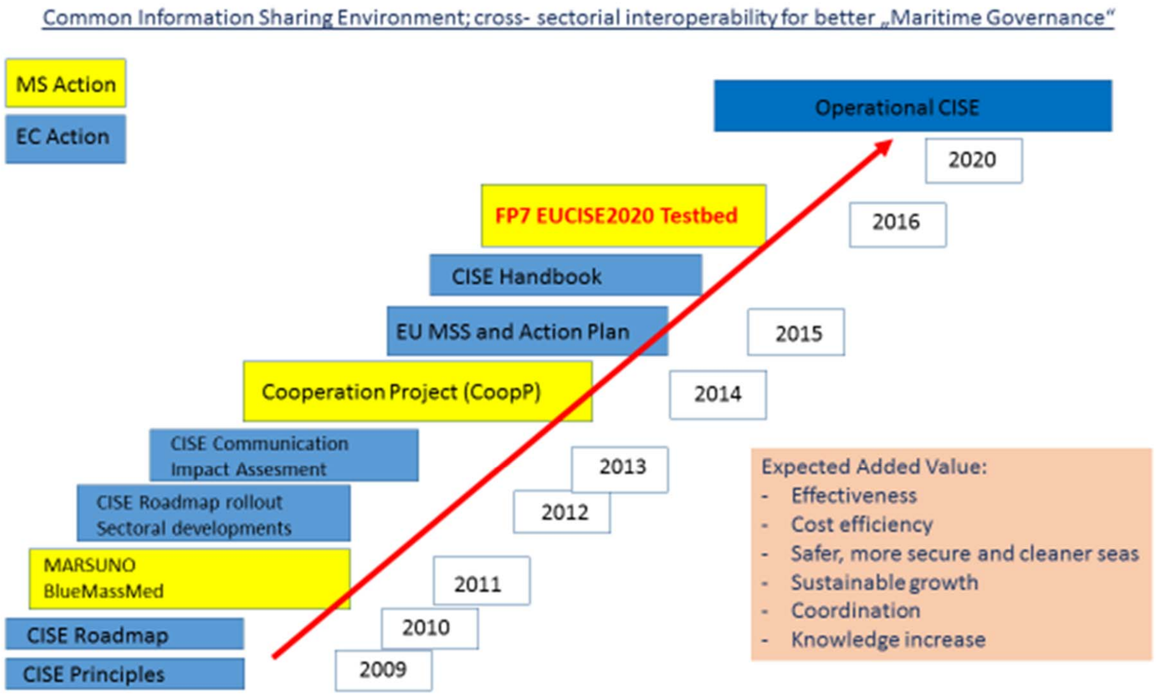

Figure 3: CISE Roadmap

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 "EUCISE2020"**, based on the 9 use cases selected, defined the requirements for and developed the common architecture of the CISE information exchange network. Consequently, a total of 11 so- called "CISE Nodes" were built, integrated and successfully tested in 8 European countries, connecting a total of 20 sectoral legacy systems of various nature.

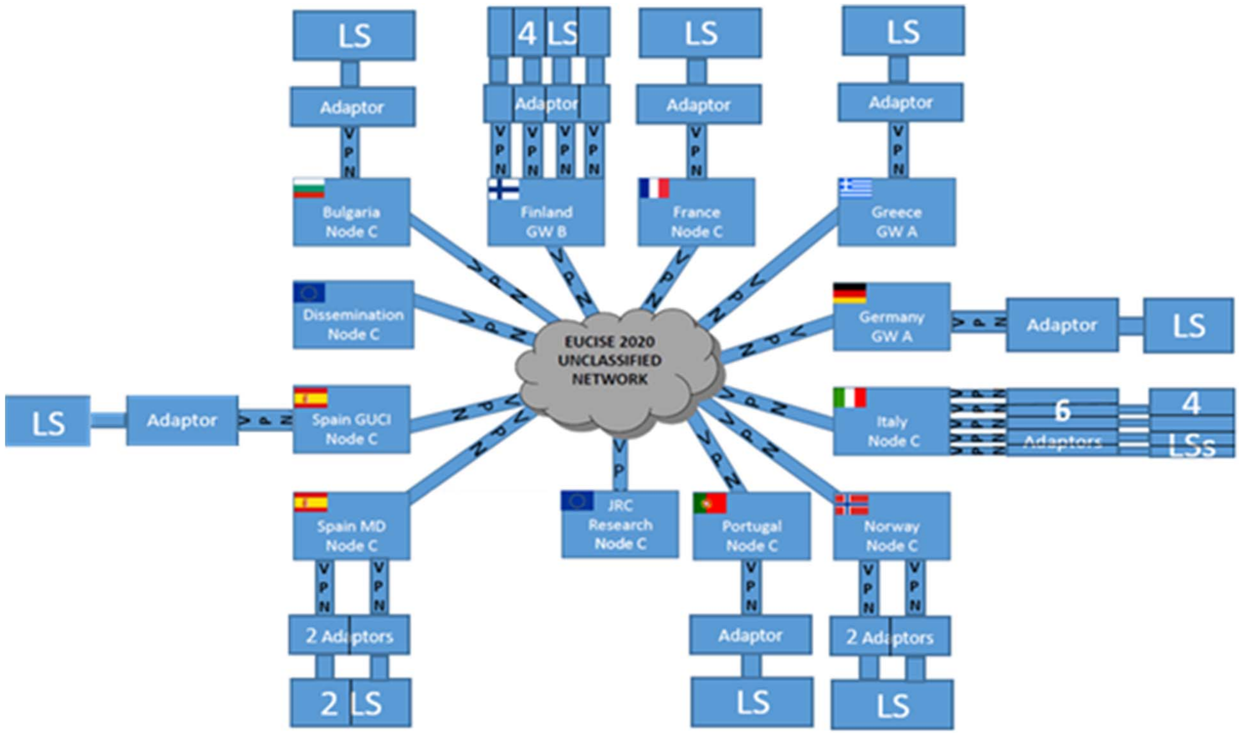

Figure 4: Diagram of the EUCISE2020 testbed set-up

The CISE network is currently able to link European countries and legacy systems of the national administrations connected to the CISE network through adapters.

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 Architecture for the European Common Information sharing environment service and Data Model (CDM).

The present document describes the following architecture:

- Infrastructure (Core Services):
  - Network and Secure Communication
  - Application Security
  - Auditing
  - Administration User Interface
  - Collaboration tools
- Interface (Common Services):
  - Consumer
  - Provider

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

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

[2] Recommendation ITU-T X-509 (10/2019): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[3] IETF RFC 793: "Transmission Control Protocol, Darpa Internet Program Protocol Specification", September 1981.

NOTE: Available at https://tools.ietf.org/html/rfc793.

[4] IETF RFC 791: "Internet Protocol, Darpa Internet Program Protocol Specification", September 1981.

NOTE: Available at https://tools.ietf.org/html/rfc791.

[5] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol", Version 1.2.

NOTE: Available at: https://tools.ietf.org/html/rfc5246.

[6] IETF RFC 6176: "Prohibiting Secure Sockets Layer (SSL)", Version 2.0.

NOTE: Available at https://www.ietf.org/rfc/rfc6176.txt.

[7] IETF RFC 6120: "Extensible Messaging and Presence Protocol (XMPP): Core".

NOTE: Available at http://xmpp.org/rfcs/rfc6120.html.

[8] IETF RFC 6121: "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence".

NOTE: Available at http://xmpp.org/rfcs/rfc6121.html.

[9] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

NOTE: Available at https://tools.ietf.org/html/rfc3550.

[10] WebRTC 1.0: "Real-Time Communication Between Browsers".

NOTE: Available at https://www.w3.org/TR/webrtc/.

[11] IETF RFC 4918: "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)".

NOTE: Available at https://tools.ietf.org/html/rfc4918.

[12] IETF RFC 4791: "Calendaring Extensions to WebDAV (CalDAV)".

NOTE: Available at https://tools.ietf.org/html/rfc4791.

[13] IETF RFC 6638: "Scheduling Extensions to CalDAV".

NOTE: Available at https://tools.ietf.org/html/rfc6638.

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, Version 3.00, 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).

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

[i.4] W3C® Recommendation XML Signature Syntax and Processing Version 2.0.

NOTE: Available at https://www.w3.org/TR/xmldsig-core2/.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

access right matrix: tool used to link each service and entity provided by Participants on the Node with all the possible consumers

NOTE: It ensures that a service is not available to all the Participants belonging to a given Community or that one of the entity's attributes exchanged by the service is not allowed to a given Participants and need to be removed by the response provided by the service.

activity: activity performed by a sector

adaptor: component external to CISE network connecting a Participant to CISE network via standardized interface

NOTE 1: The Adaptor is the bridge between the Legacy System and the Gateway translating LS data to the CISE Data Model. The Adaptor uses available Gateway Services depending on the strategy chosen for message exchange patterns and Data Model.

NOTE 2: The Adaptor could be either software or software/hardware component.

NOTE 3: In case of a new system connected to CISE, the Adaptor functionality may be part of the new system.

Certification Authority (CA): entity issuing digital certificates, authenticating the ownership of a public key by the named subject of the certificate

classified: sensitive information to which access is restricted by law or regulation

consumer: participant requesting Services 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

NOTE: See https://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance_en for more information.

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

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

EUCISE2020: 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.

NOTE 1: EU classified information is any information or material designated by the EU security classification, the unauthorised 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 unauthorised 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 unauthorised 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 unauthorised 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 unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

information system: system designed to collect, process, store, and distribute information

Legacy System (LS): 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, Public Authorities maintain Legacy Systems. 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.

national information system: information system related to the specific Member State.

node: software components that provide CISE infrastructure and access point to CISE network.

node administrator: role assumed by a User to manage the 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.

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

participant: Legacy System (LS) connected to the CISE network for exchanging data supporting one or more of the seven sectors in performing their Activities

provider: participant providing Services over CISE network

public authority: any organisation 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 organisation may have responsibilities linked to one of the seven sectors of maritime surveillance.

public key certificate: digital certificate or identity certificate used in cryptography as an electronic document to prove the ownership of a public key

NOTE 1: The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified that the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

NOTE 2: A Public Key Infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates. The PKI creates digital certificates that map public keys to entities.

NOTE 3: In a typical public-key infrastructure (PKI) scheme, the signer is a Certification Authority (CA).

regional information system: information system related to a specific Area (region)

sector: user community involved in maritime surveillance

NOTE: The seven sectors are the following:

- Maritime Safety, Security and Prevention of Pollution by Ships
- Fisheries Control
- Marine Pollution Preparedness and Response, Marine Environment
- Customs
- Border Control
- General Law Enforcement