Common information sharing environment service and Data Model (CDM); Analysis for the specifications of a testing suite for the Common Information Sharing Environment (CISE); Preliminary analysis

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.
Contents

Intellectual Property Rights ........................................................................................................... 4
Foreword ........................................................................................................................................... 4
Modal verbs terminology .................................................................................................................. 4
Executive summary .......................................................................................................................... 4
Introduction ....................................................................................................................................... 5

1 Scope ........................................................................................................................................... 7

2 References ..................................................................................................................................... 7
2.1 Normative references ............................................................................................................... 7
2.2 Informative references ............................................................................................................ 7

3 Definition of terms, symbols and abbreviations ......................................................................... 8
3.1 Terms .......................................................................................................................................... 8
3.2 Symbols ....................................................................................................................................... 9
3.3 Abbreviations ........................................................................................................................... 9

4 Description of the IUT .................................................................................................................. 10
4.1 Overview ................................................................................................................................... 10
4.2 CISE Node internal structure ................................................................................................. 11
4.3 CISE Node-to-Node interface ................................................................................................. 12
4.4 CISE Adaptors ........................................................................................................................ 12

5 The testing environment .............................................................................................................. 13
5.1 Overview ................................................................................................................................... 13
5.2 Lightweight testing box ......................................................................................................... 14
5.3 The ETSI CDM testing platform ............................................................................................ 14

6 Conformance testing .................................................................................................................... 15
6.1 Functional requirements to be tested .................................................................................... 15
6.2 Test Suite Structure (TSS) and Test Purposes (TP) ............................................................... 16
6.3 Abstract Test Methodology (ATM) and Test Generation ....................................................... 17

7 Interoperability testing ............................................................................................................... 18
7.1 Functional requirements to be tested .................................................................................... 18
7.2 Protocols to be tested ............................................................................................................. 19

8 Final Recommendations ............................................................................................................. 19

Annex A: Installing the "Lightweight testing box" ......................................................................... 20
A.1 Downloading CISESIM VM ................................................................................................. 20
A.2 Checking VM behaviour ........................................................................................................ 20
A.2.1 Process status ..................................................................................................................... 20
A.2.2 Sending and receiving messages from command line .................................................. 21
A.2.3 Sending and receiving messages from the AIS adaptor ................................................ 22

Annex B: CDM Test Purpose example .......................................................................................... 23
B.1 Message Format ..................................................................................................................... 23
B.2 Message HTTP request from the Adaptor .......................................................................... 23
B.3 Message Payload from the receiver node (CISE simulator) .............................................. 24

History ............................................................................................................................................. 26
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™, PLUGTESTSTM, UMTSTM, 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 Report (GR) 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 "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.

Executive summary

In the present document Testing and Validation for the software implementation of candidate CISE nodes and adaptors is addressed. The present document sets the bases for a comprehensive definition of the Test Cases and Testing Methodology to assess conformance and interoperability and contains the preliminary recommendations for the development of a Test Suite and a Testing Platform hosting the Software Implementation Under Test together with the necessary ICT tools and resources.

This work has to be considered preliminary and should be finalized by a Future Work aimed at addressing analytically all the recommendations included hereby.
Introduction

The CISE network is a Peer-to-Peer architecture connecting public authorities and their (legacy) IT systems responsible for maritime surveillance. The adaptor role is to connect seamlessly the Legacy System to the CISE network.

![Figure 1: The CISE peer-to-peer architecture](image)

ETSI ISG CDM has accomplished an initial standardization of all specifications needed to implement a CISE node and a set of adaptors connecting with legacy systems maintained by the Member States. All informative references are included in the present document.

To properly qualify a certain implementation of the CISE node and its adaptors based on the specifications coming from ETSI ISG CDM set of standards, it is necessary to refer to ETSI documents published by the Methods for Testing and Specification (MTS) technical committee.

As from the Conformance Testing [i.1], it is necessary to define the boundaries for testing so that the Implementation Under Test (IUT) is separated from the Test System as shown in Figure 2.

The points where the tester controls and observes the IUT are called the Points of Control and Observation (PCO).

![Figure 2: How to design a testing system for conformance testing using ETSI formal methodology (from ETSI ETS 300 406 [i.1])](image)
The product tests are performed on open standardized interfaces in order to let the Test System correctly interact with the Product. A comprehensive testing methodology consists of three complementary parts:

- Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma;
- Test Suite Structure and Test Purposes (TSS & TP);
- Abstract Test Methodology (ATM) and Test Suite implementation.

As shown in Figure 2, it is assumed to rely on a comprehensive set of Base Standards so that it will be possible to technically define the IUT and its interfaces. The Implementation Under Test (IUT) can include either the “Node” functional block including eventual interfaces with adaptors or the adaptors themselves.

Aiming at the deployment, in the present document an actual technical design of a dedicated Testing Platform together with its relations with a CISE testing and operational network is proposed as represented in Figure 3.

Figure 3: The prospected qualification process of the CISE Nodes and Adaptors
1 Scope

The present document provides a preliminary study for the development of a complete set of test specifications in order to enable interoperability among CISE instances.

In each clause after a high-level description of the standardized specifications, a recommendation to properly address the testing specification activity is given including the recommended implementation of the ETSI CDM Testing Platform.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 ETS 300 406 (April 1995): "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[i.2] ETSI EG 202 810 (V1.1.1): "Methods for Testing and Specification (MTS); Automated Interoperability Testing; Methodology and Framework".

[i.3] ETSI GS CDM 002 (V1.1.1): "Common information sharing environment service and Data Model (CDM); System Requirements definition".

[i.4] ETSI GS CDM 003 (V1.1.1): "Common Information sharing environment service and Data Model (CDM); CDM Architecture".

[i.5] ETSI GS CDM 004 (V1.0.0): "Common information sharing environment service and Data Model (CDM); Service Model".

[i.6] ETSI GS CDM 005 (V1.5.3): "Common information sharing environment service and Data Model (CDM); Data Model".


[i.9] ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[i.10] ETSI ES 201 873-1: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language".

[i.11] ETSI ES 201 873-5: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 5: TTCN-3 Runtime Interface (TRI)".
3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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.

CISE operational network: network of CISE nodes operated by Member States

CISE testing network: official network used to qualify Nodes and Adaptors in the CISE Transition Phase

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/.

future work: comprehensive analysis of testing requirement, preparation of test specifications, and development of a Testing Suite

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

participant: Legacy System 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 (PA): 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.
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;
- Defence.

service: formalized way to exchange information between Participants 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:

- ADP: CISE Adaptor
- AIS: Automatic Identification System
- ASN: Abstract Syntax Notation
- ASN.1: Abstract Syntax Notation One
- ATM: Abstract Test Methodology
- BINO: Behavioural Inopportune event tests
- BIT: Basic Interconnection Tests
- BV: Behavioural Valid event tests
- CDM: Common information sharing environment service and Data Model
- CISE: Common Information Sharing Environment
- CSG: CISE Stakeholder Group
- DB: Data Bases
- DMZ: Dead Military Zone
- EEA: European Economic Area
- EFCA: European Fisheries Control Agency
- EMSA: European Maritime Safety Agency
- EU: European Union
- EUCISE2020: European Union Common Information Sharing Environment
- GUI: Graphical User Interface
- HTTP: Hypertext Transfer Protocol
- ICT: Information & Communication Technology
- IDL: Interface Description Language
- IT: Information Technology
- IUT: Implementation Under Test
- JSON: JavaScript Object Notation
- LS: Legacy System
- LT: Lower Tester
- MS: Member State
- MTS: Methods for Testing and Specification
- NMEA: National Marine Electronics Association
- NOD: CISE Node
- OS: Operating System
- (P)ICS: (Protocol) Implementation Conformance Statement
4 Description of the IUT

4.1 Overview

The CISE node is a distributed system protected behind a firewall. Apart from CISE specific services the node relies on generic services (like Network Adaptation via proxy, PKI, DB, Firewall, etc.) and admin services. An example of a possible CISE node implementation is shown in Figure 4.

![Figure 4: A possible configuration of the CISE node behind a firewall](image-url)
The Business Logic functionalities are described in ETSI GS CDM 003 [i.4] and can be classified into Core and Common services:

- Core services provide common facilities and enable the connection of the Participants through the Network.
- Common services include capabilities to exchange information in the network using the CISE Data and Service models.

The IUT should consist of one or both the following components:

- set of core and common services as described in clause 4.2 and clause 4.3;
- one or more Adaptors as described in clause 4.4.

### 4.2 CISE Node internal structure

Node core services include ([i.4]):

- Auditing Services:
  - Logging, Monitoring and Accounting.
- Application Security Services:
  - Identification, Authentication and Authorization.
- Network and Secure Communication Services:
  - Service Manager and Network.
- Administration User Console.
- Collaboration tools.

A node is fully functional when a certain subset of these services is enabled.

To properly define the IUT structure the following services (see clause 5.3 in ETSI GS CDM 003 [i.4]) should be selected as a minimum:

- The Auditing Services limited to accounting.
- The Application Security Services.
- The Network and Secure Communication Services.
4.3 CISE Node-to-Node interface

![Diagram showing CISE Node-to-Node interface]

Figure 5: The CISE node external interfaces to be used for testing

The Common Services are organized in Consumer/Provider functional blocks supporting the following business functions:

- Push.
- Push to unknown.
- Pull (Pull Request and Pull Response).
- Pull to unknown.
- Publish/Subscribe.

In addition to the services listed above, the Node-Node interface allows the synchronization of the service registry, the participant registry and the security certificates.

As for the case of the IUT internal structure, the node is fully functional when a certain subset of these services is enabled. To properly define the IUT structure, this subset needs to be selected according to the following recommendations:

- it is required to select at least one Service Type, e.g. Vessel Service or Incident Service;
- it is required to test at least one among the following patterns: Publish/Subscribe, Pull, Push.

The output of testing will be to qualify the IUT for the selected subset of exchange patterns and service types (e.g. Publish/Subscribe of Incident Services).

4.4 CISE Adaptors

As presented in the Introduction, the Adaptor is a bridge between the Legacy System (LS) and the CISE Node, implemented according to the CDM specifications. The Adaptor is responsible for the communication and data exchange between these two systems. To support that responsibility, the Adaptor is made of two main components:

- the CISE Service and a CISE client to communicate with the CISE Node;
- an LS Custom Service and an LS Custom client to communicate with the LS.
A typical configuration consists in Maritime Surveillance LS connected to the CISE Node in order to consume or provide different services.

Figure 6: Four possible configurations of the CISE adaptors according to CDM standards [i.4]

The Adaptor can entirely represent or be part of the IUT. It is a matter of the implementation choice to merge the adaptor into the Legacy System. The Custom interface of the adaptor is not part of the IUT whereas the CISE Message Service is the actual focus of the testing activity.

Figure 7: The interface between the Legacy System, the Adaptor, and the Node

A set of functions, complying with the Service Model, managing queries (sending data and discovering services), acknowledgements, etc., is expected to be selected. With testing the Adaptor (part of the IUT) will be qualified for the subset of the exchange patterns and service types (e.g. Publish/Subscribe of Incident Services) that will be selected.

5 The testing environment

5.1 Overview

The implementer providing a candidate IUT will be asked to retrieve the testing environment described in clause 5.2 and to connect to the testing network described in clause 5.3.
5.2 Lightweight testing box

The purpose of setting up the "Lightweight testing box" is to check the compliance of the IUT against the specifications detailed in [i.3], [i.4], [i.5] and [i.6].

The testing box is expected to be shaped as a VM (in multiple formats), developed by the European Commission's Joint Research Centre, and adapted as a working tool for the Testing Platform. It basically features the operating system and the run-time environment needed to the CISE Simulator application (CISE Sim). It also includes a sample adaptor for the AIS service.

It will be possible to use the CISE Sim application for sending and receiving CISE messages to/from newly developed CISE Nodes, adaptors (the appointed IUT described in clause 4) or other CISE Sims. The messages managed by the CISE simulator follow the data model standardized in ETSI GS CDM 004 [i.5] and the protocol standardized in ETSI GS CDM 005 [i.6].

The CISE Sim features the following functionality:

- send CISE messages using a template (from a node);
- send specific VesselService messages from the AIS adaptor;
- receive CISE messages;
- store sent/received messages;
- display the message history and the message threads (messages chains);
- discover CISE services from a CISE Node.

Through this tool it is possible to check the compliance with the specifications listed in [i.3], [i.4], [i.5] and [i.6] following the provisions described in clause 6.

A practical how-to is included in Annex A.

5.3 The ETSI CDM testing platform

The EUCISE2020 collaboration has succeeded in the full implementation and validation of a reference node, complying with the specifications described in [i.3], [i.4], [i.5] and [i.6], and allowed the deployment of 10 CISE nodes by 9 EEA Member States: Finland, Germany, Norway, Portugal, Bulgaria, France, Greece, Italy and Spain (2 nodes), and 2 more nodes deployed by EU agencies: EMSA and EFCA. The total number of adaptors is 19 connecting a set of 17 national legacy systems. This network is considered as pre-operational.

As from April 2019, EMSA is engaged in setting up and enabling, in close coordination with the Member States, the Transitional Phase, ensuring a coherent evolution of the CISE network and to achieve an operational CISE. In February 2021 the CISE Stakeholder Group (CSG) has recommended to set up a CISE testing network to qualify candidate CISE nodes under test before releasing and installing them into the operational network.

In this work it is recommended to design and implement a complementary testing platform (hereafter referred to as ETSI CDM testing platform) open to other players (e.g. firms, research organizations, institutional bodies) as IUT providers. This allows to connect their candidate IUTs and validate them against the compliance and interoperability requirements discussed in the following clauses 6 and 7. Through a firewall it will be possible to connect the IUT with the CISE testing network setting up a site-to-site VPN connection (see Figure 8).
The intention is that of allowing candidate nodes and/or adaptors having passed the tests to enter the CISE Testing Network. Adopting the prescriptions in force in CISE these assets will be finally deployed in the CISE operational network finalizing the qualification process supervised by ETSI (for compliance and interoperability) and EU (for the regulatory framework).

6 Conformance testing

6.1 Functional requirements to be tested

The Protocol Implementation Conformance Statement (PICS) pro forma is a questionnaire designed by the conformance test suite specifier [i.7]. The target of the Future Work will be that of making available one or more Protocol Implementation Conformance Statements (PICS) related to the IUT internal and external structure described in clauses 4.1 and 4.2.

The PICS is subdivided into subclauses for the following categories of information:

- guidance for completing the ICS pro forma;
- identification of the implementation;
- identification of the base standards;
- global statement of conformance;
- subclauses (depending on the considered feature);
- PICS pro forma tables.

The PICS pro forma will be formatted in accordance with the guidelines presented in ISO/IEC 9646-7 [i.9].

Some examples about the role, the functions to be implemented, and the security requirements to be implemented by the IUT provider are given in Table 1 to Table 3.
Table 1: IUT role

<table>
<thead>
<tr>
<th>Item</th>
<th>Type</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Node XX</td>
<td>XX</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Adaptor YY</td>
<td>YY</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: 1&2 OR 1&!2 OR !1&2.

Table 2: Functions

<table>
<thead>
<tr>
<th>Item</th>
<th>Type</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Accounting REST Service</td>
<td>[i.4], clause 5.3.2.2</td>
<td>c.example</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

c.example if 1/1 then m else n/a.

Table 3: Security mode (if any)

<table>
<thead>
<tr>
<th>Item</th>
<th>Type</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>X.509 certificate</td>
<td>[i.4], clause 5.3.1.3.1</td>
<td>M</td>
<td></td>
</tr>
</tbody>
</table>

6.2 Test Suite Structure (TSS) and Test Purposes (TP)

A Test Purpose (TP) is a text description of a well-defined objective of testing. Applying to conformance testing, it focuses on a single conformance requirement or a set of related conformance requirements from the base standards, formalized in the PICS. The organization of the test purposes in groups is named "Test Suite Structure". The development of the test purposes follows the analysis of the conformance requirements, clearly expressed in the base standards.

Since the set of features to be tested is not defined yet, the definition of the TSS is beyond the scope of the present document. Nonetheless it is suggested to follow the recommendations given in clause 4 and to prepare a rank-3 tree (root/class/group/category) with the root defined as CDM. The groups will be those mapping the CISE node internal structure described in clause 4.2 and the adaptor interface presented in clause 4.4 whereas the category of tests will follow the classification in ISO/IEC 9646-1 [i.7]. It will be possible to adopt a naming scheme as the one reported in Table 4 (the types of testing suggested in this table - Behavioural and Basic Interconnection tests - are just examples).
Table 4: TP naming convention

<table>
<thead>
<tr>
<th>Identifier:</th>
<th>TP/&lt;root&gt;/&lt;cl&gt;/&lt;gr&gt;/&lt;x&gt;/&lt;nn&gt;/&lt;v&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;root&gt; = root</td>
<td>CDM</td>
</tr>
<tr>
<td>&lt;cl&gt; = class</td>
<td>NOD                Node tests</td>
</tr>
<tr>
<td></td>
<td>ADP                Adaptor tests</td>
</tr>
<tr>
<td>&lt;gr&gt; = group</td>
<td>GR1</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>GRX                 Test X related to Accounting, Core, or Common functionality</td>
</tr>
<tr>
<td>&lt;x&gt; = type of testing</td>
<td>BV     Behaviour: Valid event tests</td>
</tr>
<tr>
<td></td>
<td>BINO                Behaviour: Inopportune event tests</td>
</tr>
<tr>
<td></td>
<td>BIT                 Basic Interconnection Tests</td>
</tr>
<tr>
<td>&lt;nn&gt; = sequential number</td>
<td>01 to 99</td>
</tr>
<tr>
<td>&lt;v&gt; = variant</td>
<td>01 to 99</td>
</tr>
</tbody>
</table>

To avoid an update of all TPs when the PICS document is changed, Table 5 introduces mnemonics name and the correspondence with the real PICS item number. What will be mentioned in the TP will be the mnemonics name.

Table 5: Mnemonics for PICS reference

<table>
<thead>
<tr>
<th>Mnemonic</th>
<th>PICS item</th>
</tr>
</thead>
<tbody>
<tr>
<td>PICS_NOD_CORE_AUDIT_LOGGING XX1</td>
<td></td>
</tr>
<tr>
<td>PICS_NOD_CORE_APPLICATION_AUTHORIZATION_SUBSCRIPTION_&lt;SERVICE1&gt; XX2</td>
<td></td>
</tr>
<tr>
<td>PICS_NOD_CORE_NET_SERVICE-MANAGER_PUBLISH XX3</td>
<td></td>
</tr>
<tr>
<td>PICS_NOD_CORE_NET_SERVICE-MANAGER_DELETE XX4</td>
<td></td>
</tr>
<tr>
<td>... other core services</td>
<td>XX5</td>
</tr>
<tr>
<td>PICS_NOD_COMMON_SERVICE_DISCOVER XX5</td>
<td></td>
</tr>
<tr>
<td>PICS_NOD_COMMON_SERVICE_PULL_CARGO_&lt;SERVICE1&gt; XX6</td>
<td></td>
</tr>
<tr>
<td>PICS_NOD_COMMON_SERVICE_PUSH_VESSEL_&lt;SERVICE1&gt; XX7</td>
<td></td>
</tr>
<tr>
<td>... other common services</td>
<td>XX8</td>
</tr>
<tr>
<td>PICS_ADP_COMMON_SERVICE_PUSH_VESSEL_&lt;SERVICE1&gt; XX9</td>
<td></td>
</tr>
<tr>
<td>... other adaptor services</td>
<td>XXZ</td>
</tr>
</tbody>
</table>

An example of TP, a VesselService Push is reported in Annex B.

The Future Work will target the definition of certain number of TPs organized in accordance with the adopted TSS assuring an acceptable coverage of the IUT features mapped to the PICS.

6.3 Abstract Test Methodology (ATM) and Test Generation

Starting from the actual set of TPs, the last step is the derivation of an abstract test case for each TP. In this step a choice is made for a particular test method, and the restrictions implied by the environment in which testing will be carried out are taken into account. The Future Work will therefore consider the testing environment presented in clause 5.

The preparation of an Abstract Test Methodology requires to connect the IUT with the PCO. If the Adaptor and the Network Endpoint are selected, they can be seen as the Upper Tester (UT) and Lower Tester (LT) defined in ISO/IEC 9646-2 [i.8] and a simple testing topology like the "Local Single-Layer" test method can be adopted as shown in Figure 9.
7 Interoperability testing

7.1 Functional requirements to be tested

The target is to make an instance of node interoperable with other instances \cite{i.2}. Interoperability tests will be done among suppliers and among more than one supplier and the Qualified Node installed in the CISE testing network (see Figure 10 and clause 5.3).
More specifically, Interoperability Tests will check coherence between Requests and Responses in the Common Services selected by the Future Work.

EXAMPLE: For a Vessel Service, test if the vessel provided corresponds to the one requested.

Suppliers can schedule one-to-one interoperability tests.

A CISE Qualified Node can be reached from the ETSI Testing Platform to test interoperability.

This interaction will be disciplined by ETSI convenors (leasing VPN certificates) during the testing campaigns.

7.2 Protocols to be tested

The Adaptor communicates with the CISE Network (and vice versa) through the "CISE Message Service Interface" of the Node (see Figure 5) using a SOAP or REST protocol.

The Node supports both SOAP and REST protocols for the communication with the Adaptor (see specifications in clause 5.2 of ETSI GS CDM 003 [i.4]).

The topology to be used for these tests is reported in Figure 11.

![Figure 11: Peer to peer interoperability test internally to the ETSI platform.](image)

In the Future Work the protocols to be tested will be further investigated.

It will be possible to connect the Tenant-X of the ETSI CDM platform to the CISE Testing Network via VPN.

8 Final Recommendations

Prior to the definition of the actual Test Cases it is requested to properly address the topic of distinguishing mandatory from optional features offered by the CISE node and adaptor implemented from the specifications by ETSI ISG CDM.

Once the Conformance Tests are finalized and a Testing Network is implemented it is recommended to support companies engaged in the node or adaptor development announcing public test sessions like Plugtests™.

It is moreover recommended to appoint real testbeds already active in the testing domain to host the testing campaigns.
Annex A: Installing the "Lightweight testing box"

A.1 Downloading CISESIM VM

ETSI will publish a VM that will be available (with practical details) containing all needed software (alongside the necessary end-user license) for the public testing sessions.

The VM is configured to map ports to localhost (127.0.0.1) as:

- 2222 ssh
- NODE-DOCKER (CISESIM on docker image) 8200 CISESIM GUI, 8201 CISESIM Management
- NODE1 (CISESIM on filesystem) 8300 CISESIM GUI, 8301 CISESIM Management

To enter the "NODE-DOCKER", an alias is provided `cisesh` (`alias cisesh='docker exec -ti cise_cise-sim_1 /bin/bash'`); to enter the "node1" just move to ~/.cise.

To let the VM listen from the network, the default configuration has to be slightly changed.

<table>
<thead>
<tr>
<th>Folder</th>
<th>Folder in Docker</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>~/cise1/conf</td>
<td>/srv/cise-simulator/conf</td>
<td>Configuration files</td>
</tr>
<tr>
<td>~/cise1/logs</td>
<td>/srv/cise-simulator/logs</td>
<td>Logs</td>
</tr>
<tr>
<td>~/cise1/msghistory</td>
<td>/srv/cise-simulator/msghistory</td>
<td>Sent/received CISE messages</td>
</tr>
</tbody>
</table>

A.2 Checking VM behaviour

A.2.1 Process status

The two simulators are already installed and running in the VM distributed by ETSI.

```
XXXX@cisetest:~/cise1$ ./sim status
/home/XXXX/cise1/tmp/sim.pid
[ok] sim is running
```

The CISE Sim will run in background (using nohup) even if the terminal session is closed.

The application log will be stored in the file ``logs/sim.log``.

```
XXXX@cisetest:~/cise1$ ./sim
Usage: sim COMMAND
sim server lifecycle manager (starting, stopping, debugging).

COMMAND

start  starts the simulator in a detached shell using nohup command.
run    starts the simulator in foreground.
stop   stops the simulator running in background.
restart  restart the simulator running in background.
debug-start  starts the simulator in a detached shell launching the application
```
in debug mode (port 9999).

debug-run starts the simulator in foreground launching the application in debug mode (port 9999).

status show the current status the simulator (started or stopped).

Figure A.1: An example of CISE Simulator for a Windows host

A simple simulation set-up can consist of a VM manager, a text terminal, and two GUIs showing the status of two instances of the built-in simulation engine. Using this setup it is possible to send and receive messages in the same host. In Figure A.1 an XML message sent by the Simulator is rendered on a web browser.

A.2.2 Sending and receiving messages from command line

As the CISE Sim exposes the following endpoints:

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http://HOST_ADDRESS:PORT/</td>
<td>Web interface (for web browsers)</td>
</tr>
<tr>
<td>http://HOST_ADDRESS:PORT/api/messages</td>
<td>REST interface (to <strong>receive</strong> CISE messages from other adaptors/nodes/CISE Sim)</td>
</tr>
<tr>
<td>http://HOST_ADDRESS:PORT/api/soap/messages</td>
<td>SOAP interface (to <strong>receive</strong> CISE messages from other adaptors/nodes/CISE Sim)</td>
</tr>
</tbody>
</table>

The CISE Sim can receive CISE messages from the REST and the SOAP endpoints at the same time.

With the command `./sim send 'filename'` it is possible to send a message contained in an XML file.

The destination is the same configured for cise-sim and message sent and ack received will be stored in the cise-sim repository directory.

Each message is stored in a single XML file, whose filename follows this pattern:

Timestamp_TypeName_Direction_Uuid
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>Timestamp when the message was processed, following the format: yyyyMMdd-HHmmssSSS</td>
</tr>
<tr>
<td>TypeName</td>
<td>Type of the message (i.e. PULLREQUEST, FORWARD, etc.). For the Acknowledge messages, SYNC are the ones received/sent synchronously after the message was sent/received</td>
</tr>
<tr>
<td>Direction</td>
<td>RECV for message received, or SENT for message sent</td>
</tr>
<tr>
<td>Uuid</td>
<td>Unique Universal Identifier (UUID)</td>
</tr>
</tbody>
</table>

**EXAMPLES:**

- 20201118-154611819_PUSH_SENT_376cb27e-6613-4421-b8b4-c5b66f2c57a7c.xml
- 20201118-154611853_SYNCACK_RECV_40d0e627-4e2b-4e4a-816-213-4b46c156.xml
- 20201118-172335244_PUSH_RECV_371f69f4-87f6-40a5-b8e4-c83115b27719.xml
- 20201118-172335278_SYNCACK_SENT_29970f33-1a66-40e4-a9a0-228c307e387b.xml
- 20201118-172928467_PULLREQUEST_RECV_5fc38a29-efd6-43b6-b411-d092f27c53c5.xml
- 20201118-172928469_SYNCACK_SENT_973270ca-e05c-4dc4-9892-bfa24b9da453.xml
- 20201118-173008196_GETSUBSCRIBERS_SENT_5e1ba713-7510-4f9b-aa49-6b2ae14fde47.xml
- 20201118-173008200_SYNCACK_RECV_9bb2e9b4-4081-41cc-989b-47423fd41be4.xml
- 20201118-180624920_PULLREQUEST_SENT_360e6c93-7c3d-46a3-b410-a27aba6dbb93.xml
- 20201118-180624922_SYNCACK_RECV_326c18a7-119f-4bab-88b3-71fdec188739.xml

### A.2.3 Sending and receiving messages from the AIS adaptor

In the VM an open-source AIS adaptor is provided. To launch the adaptor the following commands are executed:

```
$ cise-ais-adaptor-bin$ /adaptor run
```

By default the adaptor sends HTTP request to the default gateway http://localhost:8200/api/messages where a CISE Sim node will be listening.

The default AIS stream is contained in the `cise-ais-adaptor-bin/conf/example.ais.stream.txt` file.
Annex B:  
CDM Test Purpose example

B.1 Message Format

In Table B.1 an example of Test Purpose with header, reference to the Base Standard and the PICS is described.

The test objective allows to check that sender Information in the payload are those previously set.

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP/NODE/COMMON/VESSEL-SERVICE/01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test objective</td>
<td>Check that sender Information in the payload are those previously set</td>
</tr>
<tr>
<td>Reference</td>
<td>[i.5]</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_NOD_COMMON_SERVICE_PUSH_VESSEL_-&lt;SERVICE1&gt;</td>
</tr>
</tbody>
</table>

**Initial conditions**

with {
    the IUT being in the “operational stat”
}

**Expected behaviour**

ensure that {
    when {
        the IUT receives a ADP_COMMON_SERVICE_PUSH_VESSEL_-<SERVICE1> request from the adaptor
    }
    then {
        the IUT sends a valid service message
        containing PDU header
        containing ServerOperation
        indicating value “Push”
        and containing ServiceType
        indicating value “VesselService”
    }
}

The Adaptor uses the CISE Message interface to Push a sample AIS stream towards the CISE network.

The AIS input is described in clause B.2.

The message payload received by the target CISE Node is detailed in clause B.3.

B.2 Message HTTP request from the Adaptor

The NMEA string that is encoded is the following:

!AIVDM,1,1,,B,13P88o@02=OqrHM6FATwCvf08=E,0*73

The output of the Adaptor is a HTTP request to the default gateway (a CISE Sim process listening to a localhost port in our case of Lightweight toolbox discussed in clause 5.2).
B.3 Message Payload from the receiver node (CISE simulator)

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <ContextID>048af178-a7d2-44f8-a41c-e9346cad10d8</ContextID>
  <CorrelationID>29fe8551-b15f-4e6f-8d80-36da0b4d2af8</CorrelationID>
  <CreationDateTime>2021-01-04T18:54:52.984+01:00</CreationDateTime>
  <MessageID>1fb80383-ec03-4327-b521-f8ef96652b39</MessageID>
  <Priority>Low</Priority>
  <RequiresAck>false</RequiresAck>
  <Sender>
    <DataFreshness>NearlyRealTime</DataFreshness>
    <SeaBasin>Mediterranean</SeaBasin>
    <ServiceID>fr.ais-node01.vessel.push.provider</ServiceID>
    <ServiceOperation>Push</ServiceOperation>
    <ServiceType>VesselService</ServiceType>
    <Participant>
      <EndpointUrl>http://localhost:8080/api/messages</EndpointUrl>
    </Participant>
  </Sender>
  <Payload xsi:type="ns4:XmlEntityPayload">
    <InformationSecurityLevel>NonClassified</InformationSecurityLevel>
    <InformationSensitivity>NonSpecified</InformationSensitivity>
    <IsPersonalData>false</IsPersonalData>
    <Purpose>BorderMonitoring</Purpose>
    <EnsureEncryption>false</EnsureEncryption>
    <Vessel>
      <Identifier>
        <GeneratedBy>
          <AlternativeName>Organization Alternative Name</AlternativeName>
          <LegalName>Organization Legal Name</LegalName>
        </GeneratedBy>
        <UUID>235014365</UUID>
      </Identifier>
      <LocationRel>
        <Location>
          <Geometry>
            <Latitude>50.854515</Latitude>
            <Longitude>-1.3485667</Longitude>
          </Geometry>
          <LocationQualitativeAccuracy>Medium</LocationQualitativeAccuracy>
        </Location>
        <COG>127.7</COG>
        <Heading>127.0</Heading>
        <PeriodOfTime>
          <StartDate>2021-01-04Z</StartDate>
          <StartTime>17:54:52.000Z</StartTime>
        </PeriodOfTime>
        <SourceType>Declaration</SourceType>
        <SensorType>AutomaticIdentificationSystem</SensorType>
        <SOG>14.1</SOG>
      </LocationRel>
      <MMSI>235014365</MMSI>
      <NavigationalStatus>UnderWayUsingEngine</NavigationalStatus>
    </Vessel>
  </Payload>
</ns4:Push>
```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="">
      <Transform Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116">
        <xsl:stylesheet version="1.0"
            xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
            xmlns:s="http://www.w3.org/2000/09/xmldsig#">
          <xsl:strip-space elements="*"/>
          <xsl:output indent="false" method="xml" omit-xml-declaration="yes"/>
          <xsl:template match="*[not(self::s:Signature)]">
            <xsl:element name="{local-name()}">
              <xsl:apply-templates select="*|text()"/>
            </xsl:element>
          </xsl:template>
          <xsl:template match="s:Signature"/>
          </xsl:stylesheet>
        </Transform>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
    </Reference>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>21lBABidlsAmtL2oR71o2v7QsUU=</DigestValue>
  </SignedInfo>
  <Signature Discarded />
</Signature>

<DiscoveryProfiles>
  <ServiceID>eu.cise.greek.push.consumer.id2</ServiceID>
  <ServiceOperation>Push</ServiceOperation>
  <ServiceRole>Consumer</ServiceRole>
  <ServiceType>VesselService</ServiceType>
</DiscoveryProfiles>
<DiscoveryProfiles>
  <Community>FisheriesControl</Community>
  <Country>IT</Country>
  <ServiceOperation>Push</ServiceOperation>
  <ServiceRole>Consumer</ServiceRole>
  <ServiceType>VesselService</ServiceType>
</DiscoveryProfiles>
<ns4:Push>
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.1.1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>