ETSI GR CDM 008 V1.1.1 (2023-06)

GROUP REPORT

Common information sharing environment service and Data Model (CDM); Testing Platform

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

DGR/CDM-0015

Keywords

data, platforms, testing

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:
https://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 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

The ETSI CDM Testing Platform is intended to provide a testing environment for the validation of the candidate CISE adaptors and candidate CISE nodes by providing a set of software tools for conformance and interoperability testing activities.

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.

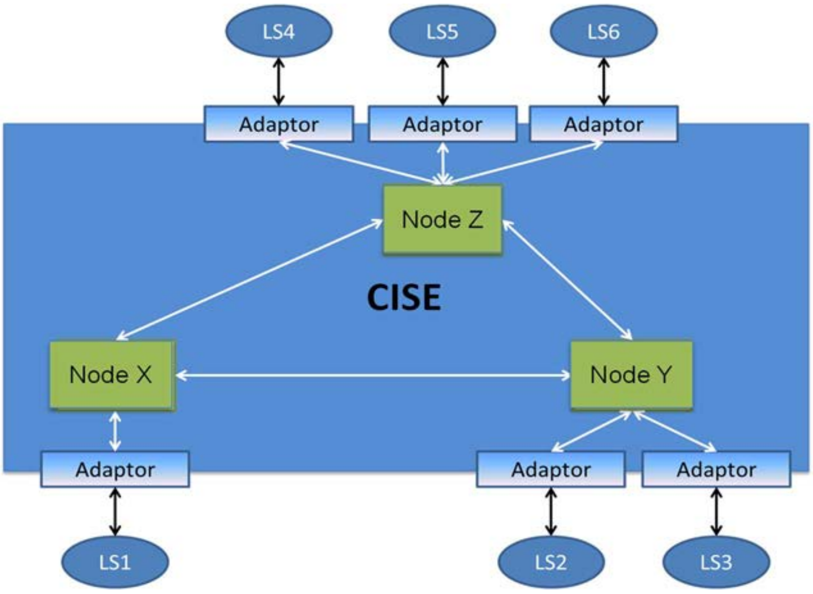


Figure 1: The CISE peer-to-peer architecture

The 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 are provided in ETSI GS CDM 004 [i.2] and ETSI GS CDM 005 [i.3].

To properly qualify a certain implementation of the CISE node and its adaptors based on such specifications, 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).

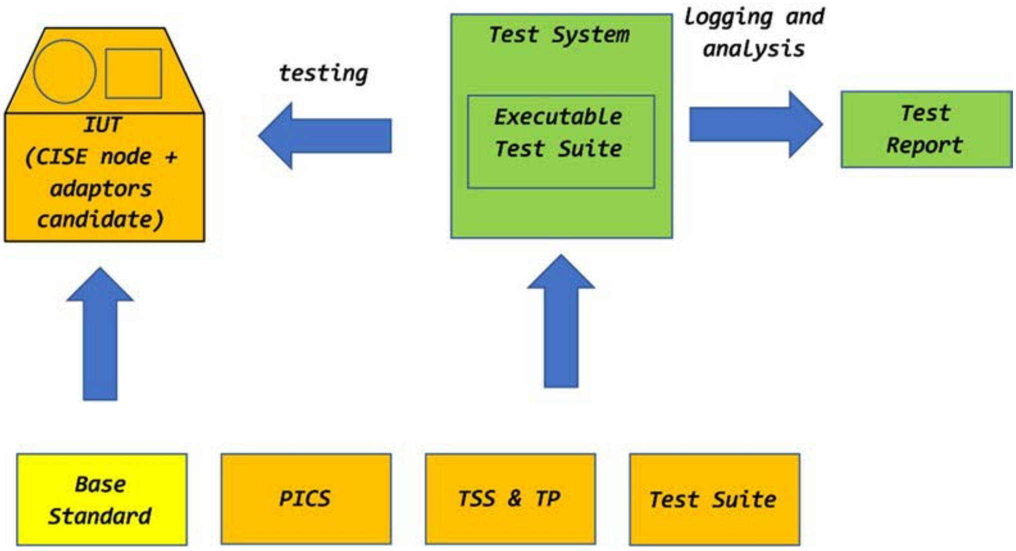


Figure 2: How to design a testing system for conformance testing using ETSI formal methodology (ETSI ETS 300 406 [i.1])

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.

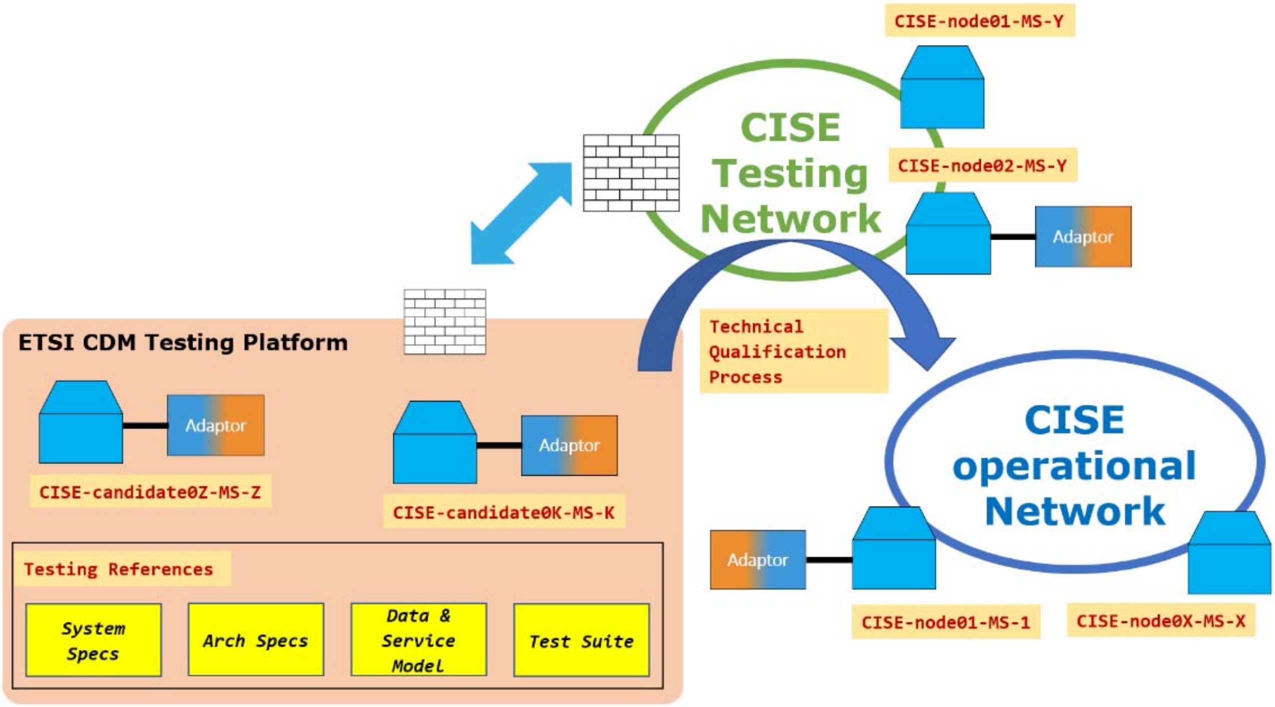


Figure 3: Prospected qualification process of the CISE Nodes and Adaptors

1 Scope

The present document provides the description of the implementation of the ETSI CDM Testing Platform for conformance and interoperability testing of the IUTs. It describes the instantiation procedures of the user tenants for testing purposes as well as the configuration of both hardware and software components.

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

[i.3] ETSI GS CDM 005 (V1.5.3): "Common information sharing environment service and Data Model (CDM); Data Model".

[i.4] 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.5] 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)".

[i.6] ETSI EG 201 015 (V2.1.1): "Methods for Testing and Specification (MTS); Standards engineering process; A Handbook of validation methods".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

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

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 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).

Representational State Transfer (REST): architectural style for providing standards between computer systems on the web It leverages the capabilities of Hypertext Transfer Protocol (HTTP) and Uniform Resource Identifiers (URIs) to retrieve or modify the state of a resource

Secure Sockets Layer (SSL): standard security technology for establishing an encrypted link between a server and a client-typically a web server (website) and a browser, or a mail server and a mail client

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

service registry: registry where services provided by the CISE Adaptors connected to a Node are registered and managed

NOTE: Each CISE Node has its own service registry.

Simple Object Access Protocol (SOAP): lightweight protocol used to create web APIs, usually with eXtensible Markup Language (XML)

tenant: group of users who share a common access with specific privileges to the software instance

Transport Layer Security (TLS): cryptographic protocol designed to provide communications security over a computer network

Virtual Machine (VM): virtual environment that functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system located on-premises

Virtual Private Network (VPN): mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet

3.2 Symbols

Void.

3.3 Abbreviations

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

AIS	Automatic Identification System
API	Application Programming Interface
ATM	Abstract Test Methodology
ATS	Abstract Test Suite
CA	Certification Authority
CDM	Common Data Model
CISE	Common Information Sharing Environment
CPU	Central Processing Unit
DBMS	Database Management System
EU	European Union
FTP	File Transfer Protocol
HDD	Hard-Disk Drive
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IMAP	Internet Message Access Protocol
IT	Information Technology
IUT	Implementation Under Test
JRC	Joint Research Center
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
LS	Legacy System
MTS	Methods for Testing and Specifications
NNTP	Network News Transfer Protocol
OS	Operating System
PaaS	Platform as a Service
PC	Personal Computer
PCO	Points of Control and Observation
PDF	Portable Document Format
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
POP	Post Office Protocol
RAM	Random Access Memory
REST	Representational State Transfer
SaaS	Software as a Service
SDN	Software Defined Network
SFP	Small Factor Pluggable
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SUT	System Under Test
TB	Terabyte
TLS	Transport Layer Security
TP	Test Purposes
TSS	Test Suite Structure

TTCN	Testing and Test Control Notation
TTCN-3	Testing and Test Control Notation 3
UNIX	Uniplexed Information and Computing Service
URI	Uniform Resource Identifier
UUID	Unique Universal Identifier
vLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
XML	eXtensible Markup Language

4 Design of the Testing Platform

4.1 General Architecture

In the present document the design and the implementation of a testing platform (hereafter referred to as ETSI CDM Testing Platform), open to all players in the CISE ecosystem (e.g. firms, research organizations, institutional bodies) as IUT providers, is described. This allows to connect their candidate IUTs and validate them against the conformance and interoperability requirements.

The intention is that of allowing candidate nodes and/or adaptors having passed the tests to enter the CISE Testing Network managed at the institutional level in the CISE transitional phase. These assets will be eventually deployed in the CISE operational network in accordance with the EU regulatory framework.

ETSI CDM Testing Platform is designed as a private cloud based on a multi-tenant infrastructure (see Figure 4). It consists of the following cloud service models:

- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).
- Software as a Service (SaaS).

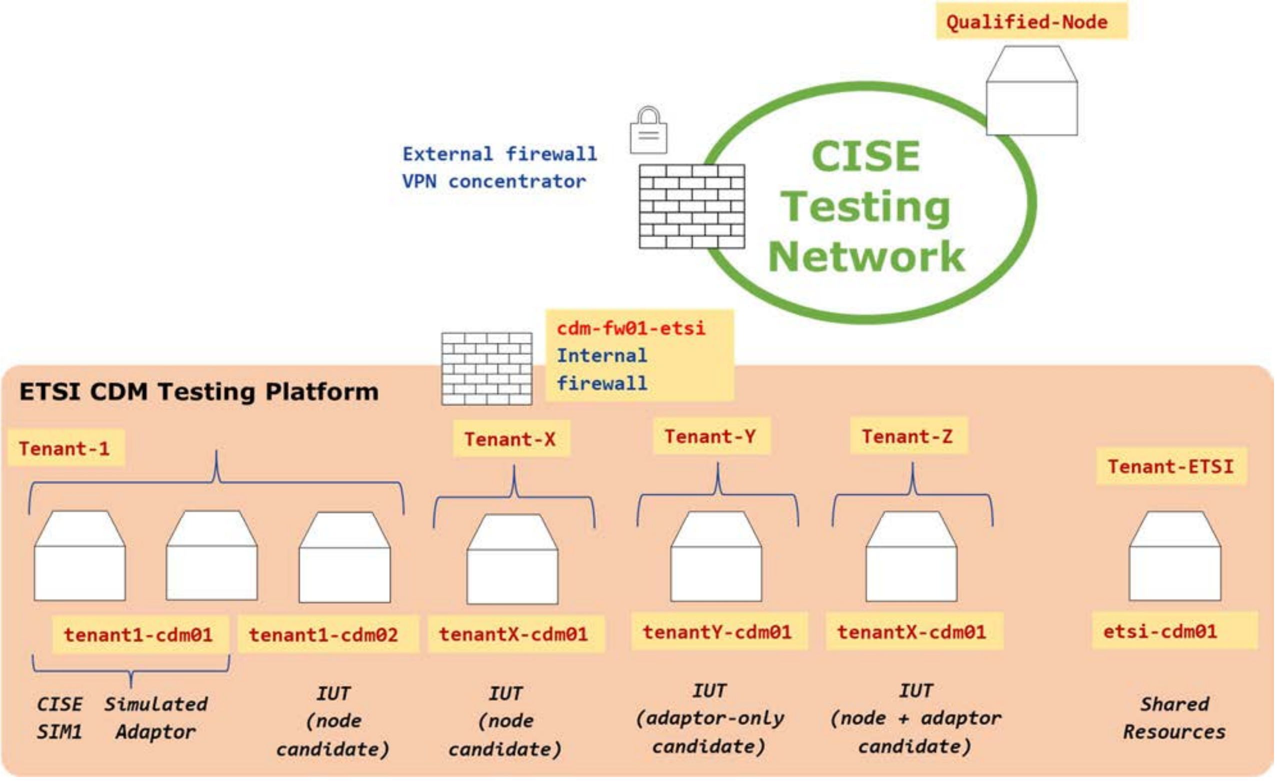


Figure 4: A conceptual scheme of the ETSI CDM testing platform

The private cloud is hosted in a physical infrastructure (dedicated server farm)**.**

4.2 Infrastructure as a Service

The server farm includes two mirrored and synchronized servers in order to prevent potential downtimes.

The infrastructure is equipped with a fiber-optic communication allowing up to 100 MBit/s data rate both in download and upload towards the Internet.

This layer provides on-demand computing resources by means of secure communications, including infrastructural components such as storage and network hardware. To fully align the ETSI CDM Testing Platform with the technical requirements coming from background experience in the CISE program, the hardware resources shown in Table 1 are allocated (single server).

Table 1: single server specifications

Server Name	Power Edge R750
CPU	Dual Xeon Gold 5317 (12 cores)
Storage HDD	4,8 TB
Storage SSD	1,9 TB
Network Adapter	Ethernet 25 Gb/s SFP+

The service allows:

- to deploy and run VMs on user tenants (see clause 5.1), including the operating system and the installed software;
- a Software Defined Networking (SDN) including software switches implementing vLANs, and custom firewall rules.

4.3 Platform as a Service

This layer provides all necessary horizontal resources to support testing processes that can be used by any user tenant:

- hypervisor services implemented with VMware ESXi technology;
- Docker as container runtime and Kubernetes as platform for dynamic management;
- network monitoring using both Zabbix and Nagios tools with templates for FTP, HTTP, HTTPS, IMAP, LDAP, MySQL, NNTP, SMTP, SSH, POP and Telnet;
- hosting and delivery of VPN services to remote and local VPN clients based on OpenVPN;
- a set of most popular DBMS and storage capabilities suited to fulfil specific user requirements;
- a local Public Key Infrastructure (PKI) to create, manage, distribute, use, store and revoke digital certificates. It binds public keys through the registration and issue of certificates by a Certificate Authority (CA). The certificates are used within the ETSI CDM Testing Platform for signing/verifying CISE messages (e.g. CISE Sim messages). The current implementation of the CA is based on OpenSSL and allows generating certificates signed by the CA.

Finally, the PaaS layer includes the Test System. The Test System is designed to check the conformance of IUT against the normative standards. The CDM Test System is described in Annex C.

4.4 Software as a Service

This layer provides a set of software and tools accessible by any user tenant, if requested. Such tools include the CISE adaptor, the CISE service registry and the CISE simulator.

The CISE adaptor allows to generate and send CISE messages. It can be used for conformance testing with a candidate CISE Node.

A generic CISE adaptor is deployed on the ETSI CDM Testing Platform permitting:

- to generate CISE messages according to the CISE Data Model, transmitted to an endpoint (either an instance of the CISE Sim or an actual CISE node);
- to consume CISE messages relayed by an instance of the CISE Sim or an actual CISE node.

The functionality of the generic adaptor is described in Annex A.

The CISE service registry is used by the CISE nodes to discover which services are provided by the CISE Adaptors and by other CISE Nodes connected via the network. They rely on a local registry.

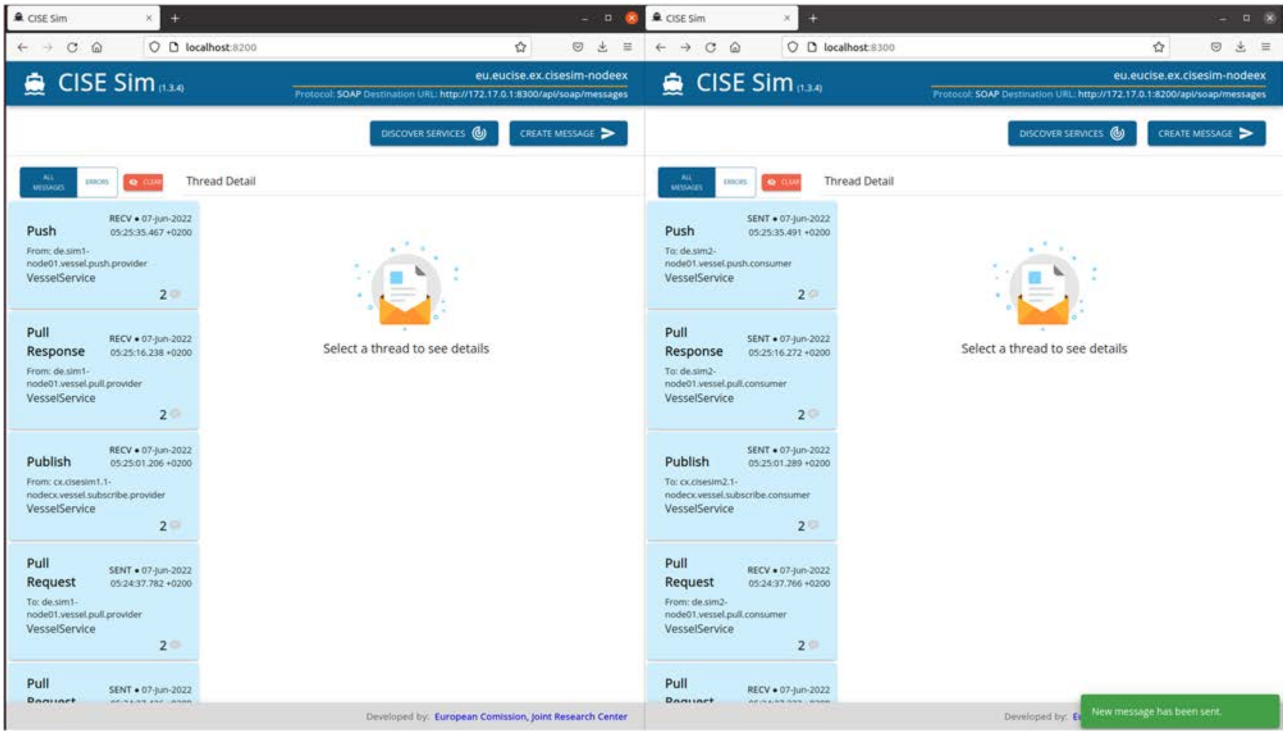
In order to be independent from the actual availability of configurable CISE Nodes in the Testing Platform and be able to consider adaptors as IUT, a local Service Registry is provided. The functionality of the service registry is described in Annex B.

The CISE simulator is an application capable of sending and receiving CISE messages to/from CISE Nodes, adaptors or other CISE simulators. The application is developed by the European Commission JRC. This software can be used by all tenants to validate an IUT against CISE Data and Service models, standardized in ETSI GS CDM 004 [i.2] and ETSI GS CDM 005 [i.3] respectively. All communication patterns for information exchange are supported: Pull, Pull Unknown, Push, Push Unknown and Publish/Subscribe. All messages can be generated using existing templates.

The CISE simulator can receive CISE messages from the REST endpoint and it is shaped as a Docker container running in a dedicated VM with the specifications in Table 2.

Table 2: VM specifications for CISE Sim

CPU	2 cores
RAM	8 GB
Storage	30 GB
OS	Ubuntu 22.04


CISE Sim
localhost:8200
CISE Sim (1.3.4)
eu.eucise.ex.cisesim-nodeex
Protocol: SOAP Destination URL: http://172.17.0.1:8300/api/soap/messages
DISCOVER SERVICES
CREATE MESSAGE
ALL MESSAGES
ERRORS
CLEAR
Thread Detail
Select a thread to see details
Developed by: European Comission, Joint Research Center
CISE Sim
localhost:8300
CISE Sim (1.3.4)
eu.eucise.ex.cisesim-nodeex
Protocol: SOAP Destination URL: http://172.17.0.1:8200/api/soap/messages
DISCOVER SERVICES
CREATE MESSAGE
ALL MESSAGES
ERRORS
CLEAR
Thread Detail
Select a thread to see details
Developed by: E
New message has been sent.

Push RECV • 07-Jun-2022 05:25:35.467 +0200
From: de.sim1-node01.vessel.push.provider
VesselService
2

Pull Response RECV • 07-Jun-2022 05:25:16.238 +0200
From: de.sim1-node01.vessel.pull.provider
VesselService
2

Publish RECV • 07-Jun-2022 05:25:01.206 +0200
From: cx.cisesim1.1-nodecx.vessel.subscribe.provider
VesselService
2

Pull Request SENT • 07-Jun-2022 05:24:37.782 +0200
To: de.sim1-node01.vessel.pull.provider
VesselService
2

Pull Request SENT • 07-Jun-2022

Push SENT • 07-Jun-2022 05:25:35.491 +0200
To: de.sim2-node01.vessel.push.consumer
VesselService
2

Pull Response SENT • 07-Jun-2022 05:25:16.272 +0200
To: de.sim2-node01.vessel.pull.consumer
VesselService
2

Publish SENT • 07-Jun-2022 05:25:01.289 +0200
To: cx.cisesim2.1-nodecx.vessel.subscribe.consumer
VesselService
2

Pull Request RECV • 07-Jun-2022 05:24:37.766 +0200
From: de.sim2-node01.vessel.pull.consumer
VesselService
2

Pull Request RECV • 07-Jun-2022

Figure 5: Example of two simulated CISE Nodes

The CISE simulator exposes the following endpoints which can be remotely invoked by any user tenant.

Table 3: List of endpoints exposed by CISE Sim

Endpoint	Description
`http://HOST_ADDRESS:8200/`	Web interface (for web browsers)
`http://HOST_ADDRESS:8200/api/messages`	REST interface (to **receive** CISE messages from other adaptors/nodes/CISE Sim)
`http://HOST_ADDRESS:8200/api/soap/messages`	SOAP interface (to **receive** CISE messages from other adaptors/nodes/CISE Sim)

CISE simulator also embeds a simple adaptor for the AIS service, supporting specific CISE VesselService messages including information imported from the AIS.

5 Tenant View

5.1 User Tenants

User tenants can be set-up on-demand by allocating all needed ICT resources, according to the requirements. A user tenant can host any IUT (either a candidate adaptor or a candidate CISE Node) or any additional tool/software for testing purposes provided by other players (e.g. firms, research organizations, institutional bodies, etc.). User tenants are remotely accessible by owners only through a VPN-based tunnelling using SSL/TLS protocol and certificates for the authentication and key exchange.

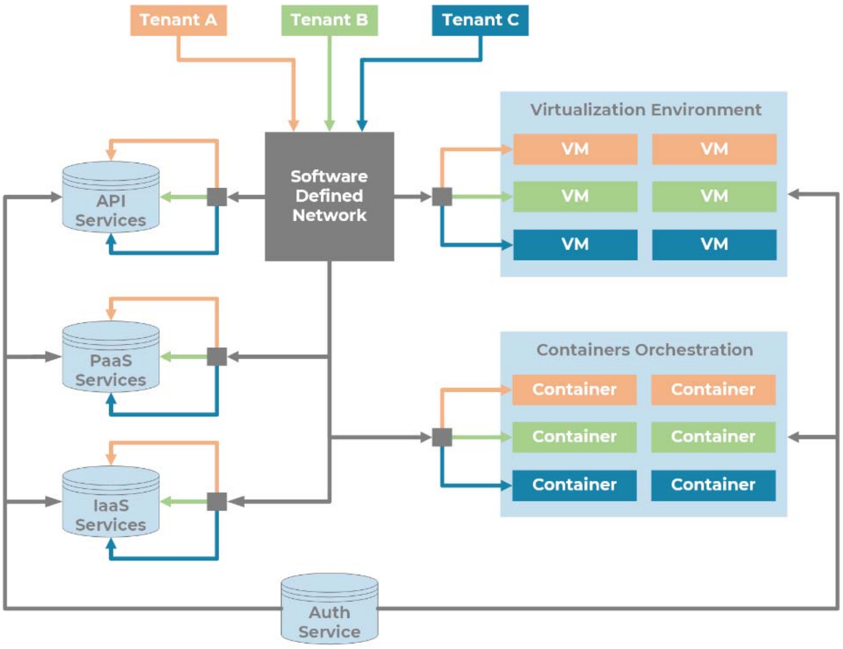


Figure 6: ETSI CDM Testing Platform multi-tenant structure

Based on requirements, user tenants could be composed by a given set of VMs with proper specifications including all needed services from the IaaS, PaaS or SaaS layers. Such services can be either standalone, provided and deployed by the tenant owner, or the shared ones provided by the ETSI CDM Testing Platform.

5.2 ETSI Tenant

This tenant is allocated to ETSI for sharing technical resources with other tenants. Such resources include:

- A Test System (see clause 4.3) to be connected with candidate IUTs.
- An instance of the CISE Adaptor (see clause 4.4).

- A CISE service registry (see clause 4.4).
- Two instances of the CISE simulator (see clause 4.4) connected one to another.

6 Conformance Testing

The aim of the conformance testing is to make the IUT (e.g. node candidate, adaptor-only candidate or node and adaptor candidates) conformant to the CISE Data and Service models. Testing and Test Control Notation (TTCN) programming language is adopted as default approach for test notation [i.4] and [i.5].

The User will be requested to connect the IUT to the Test System provided by ETSI tenant. A web interface will permit to run pre-configured tests and retrieve a Test Report.

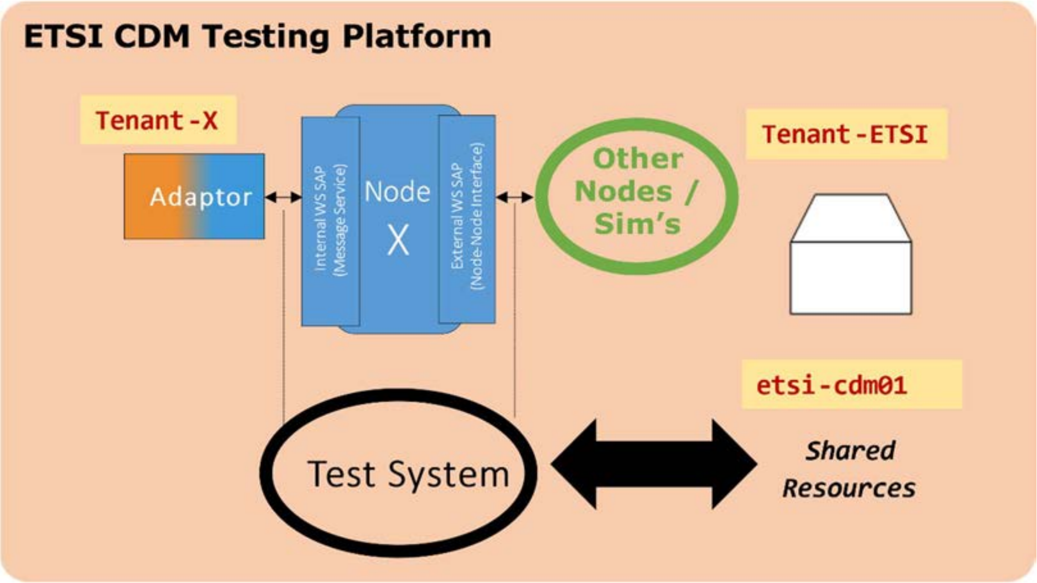

ETSI CDM Testing Platform
Tenant -X
Adaptor
Internal WS SAP (Message Service)
Node X
External WS SAP (Node-Node Interface)
Other Nodes / Sim's
Tenant -ETSI
etsi-cdm01
Test System
Shared Resources

Figure 7: Interfaces between CISE nodes and Adaptors eligible to Conformance Testing

All configurations of the Test System related to the various options of IUTs are included in Annex C.

Annex A:
CISE adaptor

CISE Adapter is responsible for receiving and processing CISE messages from the CISE system and sending them to the CISE system. To access the CISE Adaptor, the following link is provided:

- Local: http://172.25.1.58:14000/

There are two services available:

- Generate CISE Message.
- Send CISE Message.

These services are further described below.

Generate CISE Message:

[POST] /api/v1/message

This service is responsible for generating CISE messages. Those messages can be any of the following types:

- Push
- PullRequest
- PullResponse

The request will have some headers and a body. The headers can be both mandatory and optional (as described in Table A.1). The body of the request is mandatory and should be a valid JSON.

Table A.1

Name	Type	Required	Default	Example	Description
X-Message-Id	String	False	Random UUID	af7c1fe6-d669-414e-b066-e9733f0de7a8	Unique identifier of the message.
X-Content-Id	String	False	NULL	af7c1fe6-d669-414e-b066-e9733f0de7a8	Content Id of the message.
X-Correlation-Id	String	False	NULL	af7c1fe6-d669-414e-b066-e9733f0de7a8	Correlation Id of the message.
X-Creation-Date-Time	String	False	NOW	2022-01-01T00:00:00.000Z	Creation date and time of the message.
X-Priority	Enum [Low, Medium, High]	False	Low	High	Priority of the message.
X-Sender-Id	String	True	UNKNOWN	org.cise.inovaworks.push	Sender Id of the message.
X-Recipient-Id	String	True	UNKNOWN	org.cise.inovaworks.push	Recipient Id of the message.
X-Message-Type	Enum [Push, PullRequest, PullResponse, Feedback]	True	NULL	Push	Type of the message.

An example of the body of the considered request is provided hereafter:

```
{
    "type": "Vessel",
    "Identifier": {
        "GeneratedBy": {
            "type": "Organization",
            "IdentificationNumber": "inovaworks",
            "Identifier": {
                "UUID": "com.inovaworks"
            }
        },
        "UUID": "49a43ef2-42f7-4442-86f3-e1790bf273af"
    }
}
```

In addition, the following curl example can be used:

```
curl --location 'http://172.25.1.58:14000/cise-adapter/api/v1/messages' \
--header 'X-Message-Id: message-id' \
--header 'X-Context-Id: context-id' \
--header 'X-Correlation-Id: correlation-id' \
--header 'X-Creation-Date-Time: 2023-01-01T00:00Z' \
--header 'X-Priority: Medium' \
--header 'X-Sender-Id: sender-id' \
--header 'X-Recipient-Id: recipient-id' \
--header 'X-Message-Type: Push' \
--header 'Content-Type: application/json' \
--data '{
    "type": "Vessel",
    "Identifier": {
        "GeneratedBy": {
            "type": "Organization",
            "IdentificationNumber": "inovaworks",
            "Identifier": {
                "UUID": "com.inovaworks"
            }
        },
        "UUID": "49a43ef2-42f7-4442-86f3-e1790bf273af"
    },
"MMSI": 204209890
}'
```

The response is a CISE XML formatted message.

Send CISE Message:

[POST] /api/v1/message/send

This service is responsible for generating CISE messages. Those messages can be any of the following types:

- Push
- PullRequest
- PullResponse
- Feedback

The request will have some headers and a body. The headers can be both mandatory and optional (as described in Table A.2). The body of the request is mandatory and should be a valid JSON.

Table A.2

Name	Type	Required	Default	Example	Description
X-Message-Id	String	False	Random UUID	af7c1fe6-d669-414e-b066-e9733f0de7a8	Unique identifier of the message.
X-Content-Id	String	False	NULL	af7c1fe6-d669-414e-b066-e9733f0de7a8	Content Id of the message.
X-Correlation-Id	String	False	NULL	af7c1fe6-d669-414e-b066-e9733f0de7a8	Correlation Id of the message.
X-Creation-Date-Time	String	False	NOW	2022-01-01T00:00:00.000Z	Creation date and time of the message.
X-Priority	Enum [Low, Medium, High]	False	Low	High	Priority of the message.
X-Sender-Id	String	True	UNKNOWN	org.cise.inovaworks.push	Sender Id of the message.
X-Recipient-Id	String	True	UNKNOWN	org.cise.inovaworks.push	Recipient Id of the message.
X-Message-Type	Enum [Push, PullRequest, PullResponse, Feedback]	True	NULL	Push	Type of the message.

The body should be an Entity (JSON) from the CISE system (see the example below):

```
{
    "type": "Vessel",
    "Identifier": {
        "GeneratedBy": {
            "type": "Organization",
            "IdentificationNumber": "inovaworks",
            "Identifier": {
                "UUID": "com.inovaworks"
            }
        },
        "UUID": "49a43ef2-42f7-4442-86f3-e1790bf273af"
    }
}
```

In addition, the following curl example can be used:

```
curl --location 'http://172.25.1.58:14000/cise-adapter/api/v1/messages/send' \
--header 'X-Message-Id: message-id' \
--header 'X-Context-Id: context-id' \
--header 'X-Correlation-Id: correlation-id' \
--header 'X-Creation-Date-Time: 2023-01-01T00:00Z' \
--header 'X-Priority: Medium' \
--header 'X-Sender-Id: sender-id' \
--header 'X-Recipient-Id: recipient-id' \
--header 'X-Message-Type: Push' \
--header 'Content-Type: application/json' \
--data '{
    "type": "Vessel",
    "Identifier": {
        "GeneratedBy": {
            "type": "Organization",
            "IdentificationNumber": "inovaworks",
            "Identifier": {
                "UUID": "com.inovaworks"
            }
        },
        "UUID": "49a43ef2-42f7-4442-86f3-e1790bf273af"
    }
}'
```

The response is a CISE Acknowledgement.

Annex B: CISE service registry

The Service Registry provides a database for internal storage and exploration of Legacy System endpoint registrations. The following RESTful endpoints are made available on the ETSI CDM Testing Platform (http://172.25.1.58:15000/):

POST host:port/registry with a JSON data structure compliant with:

```
{
  "registration_id": 0,
  "cise_service_id": "com.company.system.entity.role",
  "description": "Description of the Service",
  "manufacturer": "Manufacturer Name",
  "endpoint_base_url": "https://localhost:8080/cise/service"
}
```

This will generate a new Service Registration and provide the caller back with the ID.

GET host:port/registry/all, will return all registered services.

GET host:port/registry/service_id?service_id=keyword, will return all registered services with keyword somewhere in the service_id.

POST host:port/admin/clear, will clear the registry's database.

Annex C:
Test System

C.1 Constraints and requirements

The purpose of the CDM test platform is to provide a reliable set of software and hardware equipment that can be used to validate TTCN-3 Abstract Test Suites (ATSs). The architecture of this test platform has been designed taking into account the following constraints:

- to be compatible with the requirements expressed in the validation handbook (ETSI EG 201 015 [i.6]);
- to be independent of the platform used to implement the test system;
- to be independent of the TTCN-3 tool provider;
- to be configurable and customizable;
- to provide tools and well defined interfaces to System Under Test (SUT), allowing test automation;
- to be easily extensible for future CDM protocols;
- to provide generic components that can be reused in other test platforms.

Test tool independence has been achieved by isolating the tool specific interfaces from core functionalities of the platform. Adapting the current platform to a different test tool would only require the implementation of a very simple piece of software mapping tool-specific functions to generic functions defined in this project. In addition, great care has been taken to separate CDM specific functionalities from generic test platform tasks in order to provide a maximum number of reusable components for future test platforms.

C.2 General architecture

Typically a TTCN-3 test platform is composed of four different components:

- The TTCN-3 test tool providing necessary software to execute the abstract test suites.
- The hardware equipment supporting TTCN-3 test execution and adaptation to SUTs.
- The codecs which convert protocol messages into their abstract TTCN-3 representation.
- The Test Adapter (TA) implementing interfaces with the device under test.

The interaction of these components is described in Figure C.1.

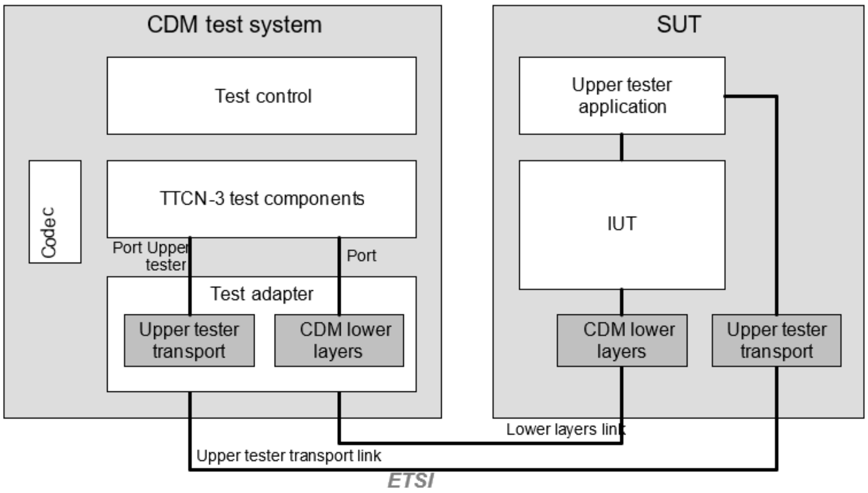


Figure C.1: Abstract protocol tester - CISE ATS

The TTCN-3 test tool is usually provided by third parties and their description is out of the scope of the present document. The implementation details of the other components are described in the present document.

C.3 CDM Test System requirements

C.3.1 Hardware

The main hardware component of the CDM test platform is a standard PC. Its role is to host the execution of the test suites using a TTCN-3 test execution tool. Whatever operating system is installed on the computer, it is necessary to ensure that the following points are taken into account:

- No firewall interference with traffic generated by the Test System and/or SUT.
- Excellent time synchronization between the SUT and the test system.

The communication between the SUT and the test system is achieved through Ethernet if the SUT supports it or using an access layer adaptation box, as shown in Figure C.2.

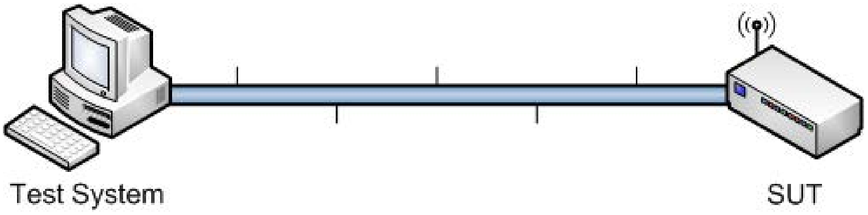


Figure C.2: Communication via Ethernet

C.3.2 Software

The ETSI CDM Test System is based on TITAN™ project [i.6] and its core components. The ETSI CDM Test System requires a UNIX®/Linux®-like environment.

NOTE: See https://projects.eclipse.org/projects/tools.titan for information on the TITAN™ project.

C.3.3 Virtualization

A dockerized version of the ETSI CDM Test System is available.

C.3.4 Continuous Integration

Located at the root of the source code architecture, a script name *.jenkins.sh* is provided in order to integrate the ETSI Test System source code in a Continuous Integration mechanism based on Jenkins®.

C.3.5 Code documentation

Based on Doxygen® a documentation in PDF can be generated.

C.4 Test Configuration

C.4.1 Introduction

This test suite uses three test configurations as defined in clauses below.

C.4.2 Config_CISE_1

The CISE node is acting as the IUT. This configuration is used to test the interface between the CISE node and the CISE Adaptor.

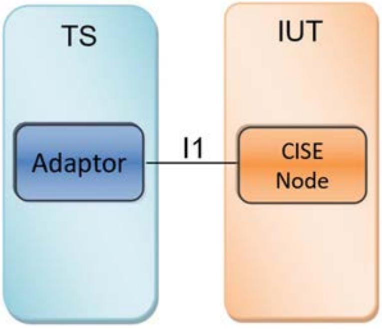


Figure C.3: Config_CISE_1 to validate interface between IUT and the CISE Adaptor

C.4.3 Config_CISE_2

The CISE node is acting as the IUT. This configuration is used to test the interface between the CISE node and the CISE Network.

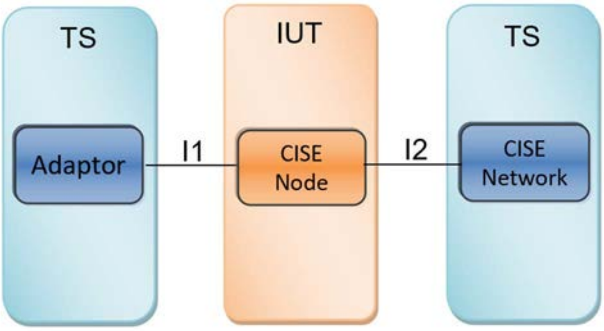


Figure C.4: Config_CISE_2 to validate interface between IUT and the CISE Network

C.4.4 Config_CISE_3

The CISE Adaptor is acting as the IUT. This configuration is used to test the interface between the CISE Adaptor and the CISE node.

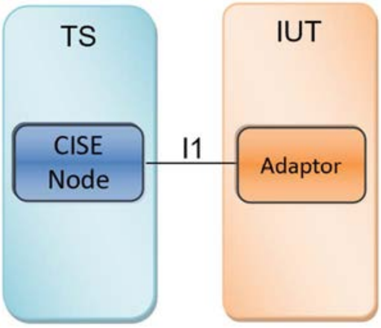


Figure C.5: Config_CISE_3 to validate interface between IUT and the CISE Node

History

Document history		
V1.1.1	June 2023	Publication