ETSI GS CDM 003 V2.1.1 (2024-08)

Common information sharing environment service and Data Model (CDM); CDM Architecture; Release 2

Disclaimer

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

Reference
RGS/CDM-0018

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

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

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

Following year, on October 2010, European Commission adopted a new CISE related Communication "Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain", which provided the plan for the first concrete actions towards building the CISE [i.2].

The Communication noted that added value of integrating maritime surveillance is to enhance the present sectoral maritime awareness pictures of the sectoral user communities, with additional relevant cross-sectoral and cross-border surveillance data on a responsibility to share basis. Such enhanced pictures would increase Member States authorities' efficiency and improve cost effectiveness. It was further noted that the decentralized information exchange system is directed to interlink all relevant user communities, taking into account existing sectoral information exchange networks and planned systems, and allowing for the improvement and development of both the existing sectoral systems, and the overarching CISE network architecture.

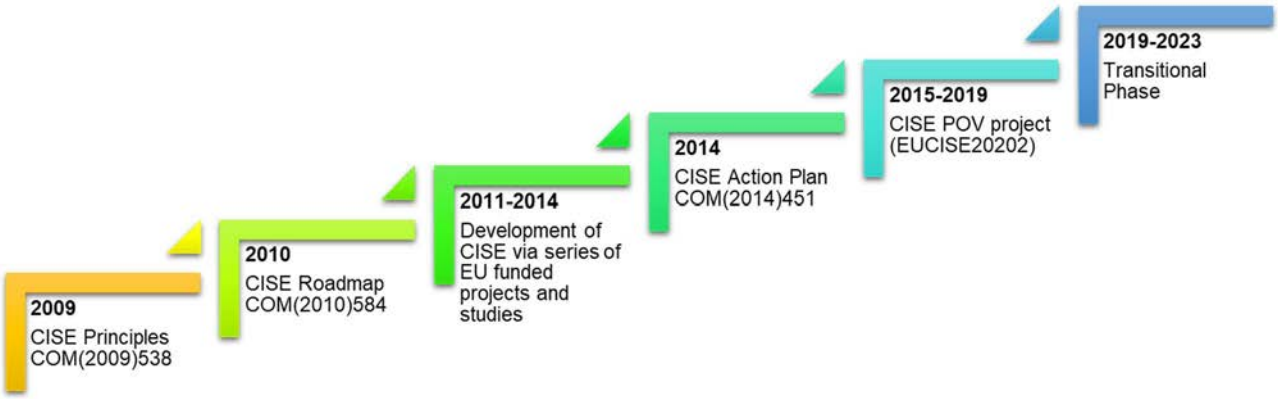


Figure 1: CISE development process

During to following years, from 2011 to 2014 a series of EU sponsored projects and studies, building up one on another and supported by JRC and the Member States Technical Advisory Group (TAG), investigated and developed the legal, organizational, semantical and technical interoperability of CISE. The CISE principles were further elaborated [i.3], and number of use cases, covering the most relevant activities of all sectors were identified. Based on these use cases, the first versions of the technical interoperability tools (e.g. data model and communication patterns) were developed.

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

The POV project "European test bed for the maritime Common Information Sharing Environment in the 2020 perspective", in short "EUCISE 2020", was launched in 2015. It defined the technical requirements, developed the common architecture and established a CISE information exchange network testbed. Consequently, a total of 12 so-called "CISE Nodes" were built, integrated and successfully tested in 9 European countries, connecting a total of 20 sectoral Legacy Systems of various nature (Figure 2).

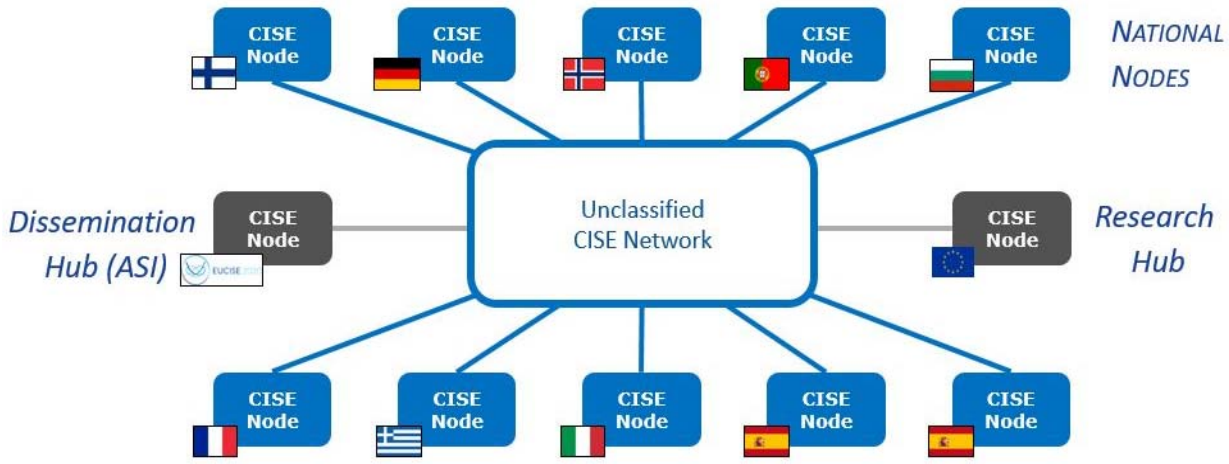
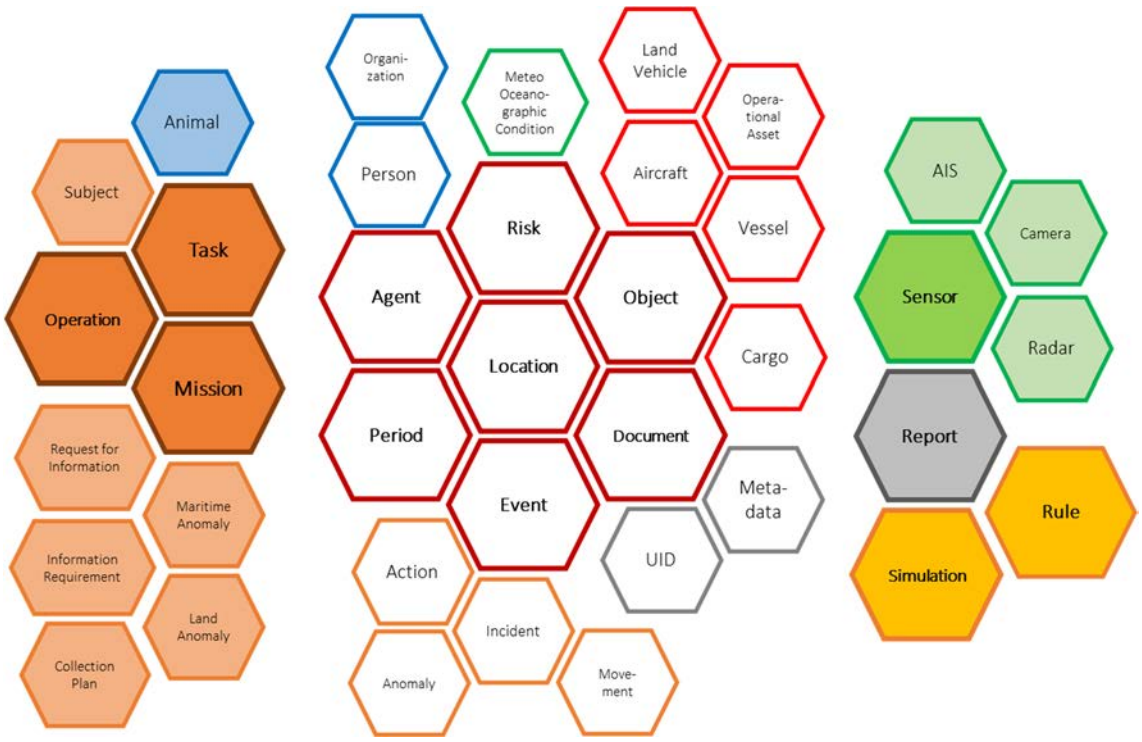


Figure 2: EUCISE 2020 testbed set- up

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

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

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



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

Figure 3: Enhanced CISE Data Model

The requirements in the present document respect the operational and technical requirements defined during the CISE development process (Figure 1) and the general principles of CISE as originally defined in [i.1], [i.3] and later elaborated in the most recent version of the CISE Architecture [i.4] as follows:

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

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

1 Scope

The present document defines the Architecture for the European Common information sharing environment service and Data Model (CDM). With the ANDROMEDA project it was proven that the CISE architecture can be used in cross-sectoral and cross-border information exchange in addition to the maritime environment.

The present document describes the architecture of the CISE node organized in three layers of functional blocks (i.e. Common, Management, and Security services). It also provides the normative behaviour of the blocks contained therein, as well as the external and internal interfaces that are requested to be implemented for conforming to such an architecture. The Adaptors are also described limiting the normative provisions to the interface exposed to the CISE Node.

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; Release 2".

[2] ETSI GS CDM 004: "Common information sharing environment service and Data Model (CDM); Service Model; Release 2".

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

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

[5] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol", Version 1.3.

[6] IETF RFC 2660: "The Secure HyperText Transfer Protocol".

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] COM/2009/538 final: "Communication from the Commission to the Council the European Parliament, the European Economic and Social Committee and the Committee of the Regions; Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain".

[i.2] COM/2010/584 final: "Communication from the Commission to the Council and the European Parliament; on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain".

[i.3] "CISE Architecture Visions Document", V3.0, 06/11/2013.

[i.4] "CISE Architecture", Version 2.0, 04/03/2022.

[i.5] COM/2014/451 final: "Communication from the Commission to the Council and the European Parliament; Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain".

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

Common Information Sharing Environment (CISE) operational network: network of CISE nodes operated by Member States

Common Information Sharing Environment (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

NOTE: In the present document, Public Authorities maintain Legacy Systems. Legacy Systems are the originator and final destinations of messages exchange through the CISE Network.

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: technical personnel in charge of managing the node's subsystems and the creation of new Adaptors

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

participant administrator: technical personnel in charge of managing a set of functionalities of the Adaptor or Legacy System

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. 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:

AAA	Authentication, Authorization & Accounting
API	Application Programming Interface
CA	Certification Authority
CDM	CISE Data Model
CISE	Common Information Sharing Environment
CPU	Central Processing Unit
EEA	European Economic Area
EI NA	External Interface Node - Adaptor
EI NN	External Interface Node - Node
EMSA	European Maritime Safety Agency
EU	European Union
EUCISE 2020	European Union Common Information Sharing Environment
GS	Group Specifications
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure

ICT	Information and Communications Technology
ID	IDentifier
II MC	Internal Interface Management services - Common services
II SC	Internal Interface Security services - Common services
IP	Internet Protocol
IPSEC	Internet Protocol SECurity
IT	Information Technology
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JRC	Joint Research Centre
LS	Legacy System
MS	Member State
PKI	Public Key Infrastructure
POV	Pre-Operational Validation
REST	Representational State Transfer
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TAG	Technical Advisory Group
TLS	Transport Layer Security
URI	Uniform Research Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UUID	Universal Unique IDentifier
VM	Virtual Machine
VPN	Virtual Private Network
XML	eXtensible Markup Language

4 Overview

The present document presents the architecture for the information sharing environment exploiting the results obtained within the EUCISE 2020 project and the subsequent CISE Transitional and Operational Phases.

Although CISE architecture has been designed for the maritime domain, the architecture described in the present document is also applicable to other domains.

CISE is designed to enable the interoperability of the Legacy Systems, national or European, belonging to public authorities in the European Economic Area. Technical and semantic interoperability is achieved through two software building blocks:

- **Node**, which is an information broker, implementing the common CISE specifications and connecting legacy systems across the EEA.
- **Adaptor**, which the information exchange between a legacy (LS) system to connect to a CISE Node. It converts the LS data into the common CISE data model. This is an optional component.

The capabilities of a CISE node can be grouped into three different service layers:

- **Common services**, dedicated to the high-level information I/O including validation.
- **Security services**, dedicated to the accounting, authentication, and authorization, as well as validation tasks and integrity checks.
- **Management services**, dedicated to enable users manage the other services of the CISE Node.

CISE Nodes can be arranged in different network topologies. Public authorities decide on the network topology and network security based on the nature of the information and the purpose of the information exchange.

CISE Nodes and Adaptors can be arranged in different organizations to simplify the connection of the legacy systems among them. Node owners decide the number of Adaptors connected to a CISE Node, their organization and how legacy systems connect to the adaptors.

In the present document, requirements are identified by a combination of abbreviated main clause name (i.e. Gen, Com, Mgt or Sec), two or three letter descriptive code (e.g. related to the clause name) and a sequential number (e.g. "Com-VAL-001" for a requirement on Message Validator from the Common Services).

5 Architecture description

5.1 Top-Level Architecture

The CISE shall allow the Legacy Systems to exchange data. The Adaptors are the components of the architecture able to translate the Legacy System communication world into the CISE network language, protocol and data model. Each Legacy System connected to the CISE network requires a specific Adaptor developed on purpose, in order to integrate its own legacy system. In case a Legacy System natively integrates the Adaptor's capabilities (e.g. supporting CISE Data and Service models), the communication between a CISE Node and the above-mentioned Legacy System does not require the implementation of the Adaptor.

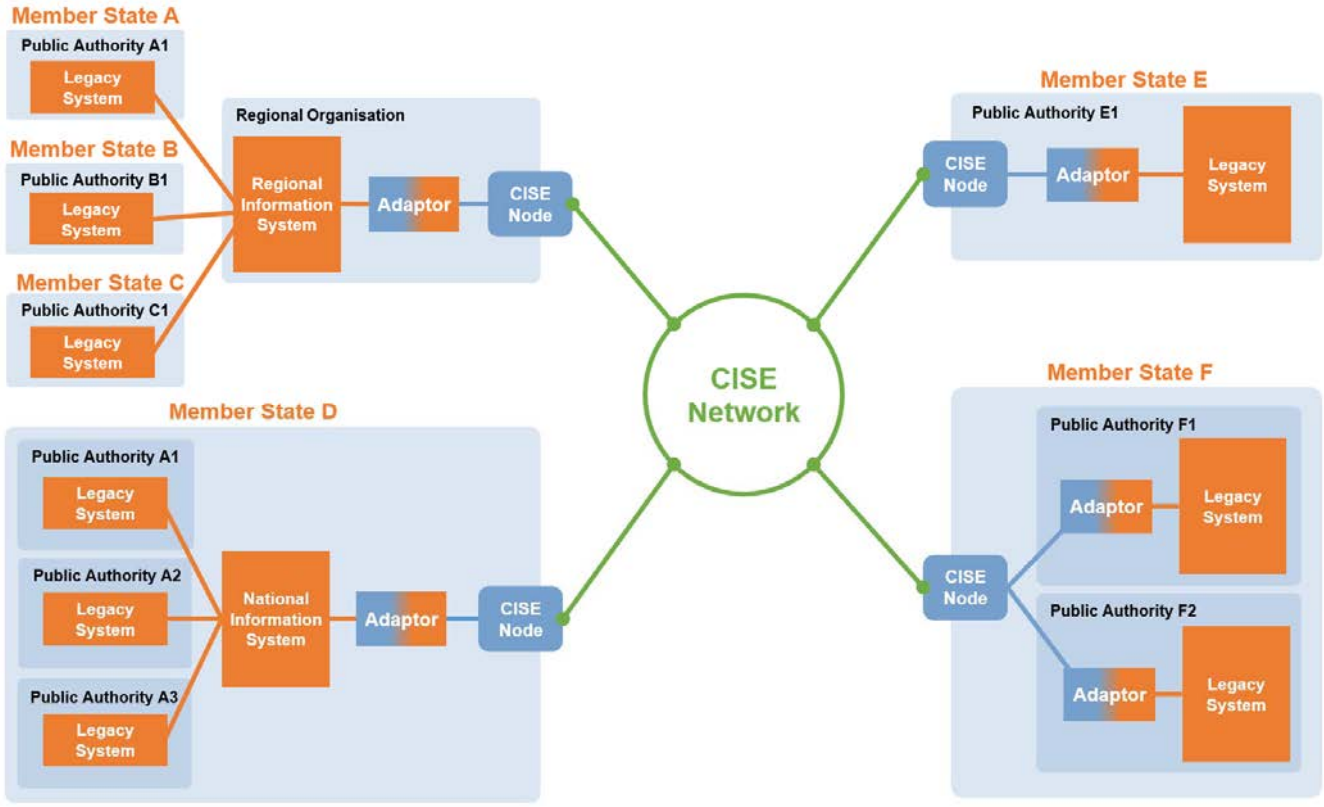


Figure 4: CISE top level architecture

Adopting one of the supported topologies (see Annex B) the overall resulting network is the one displayed in Figure 4.

5.2 Local/Regional level architecture

5.2.1 General Requirements

The MS local network shall mange the following functionalities:

- The message exchange.
- The administration of the CISE node.

As depicted in Figure 4, different configurations can be used for connecting Public Authorities and their Legacy Systems to the CISE Network.

A Legacy System (as depicted in Figure 5) might be either a legacy information system which requires the implementation of an external adaptor for the communication with a CISE Node, or a new information system which natively integrates such capabilities: in case of a new information system connected to the CISE node, the adaptor functionality shall be part of the system itself.

Without losing generality, the option associated to Public Authority E1 of the Member State E by considering Legacy System/Adaptor/Node configuration is described, as depicted in Figure 4.

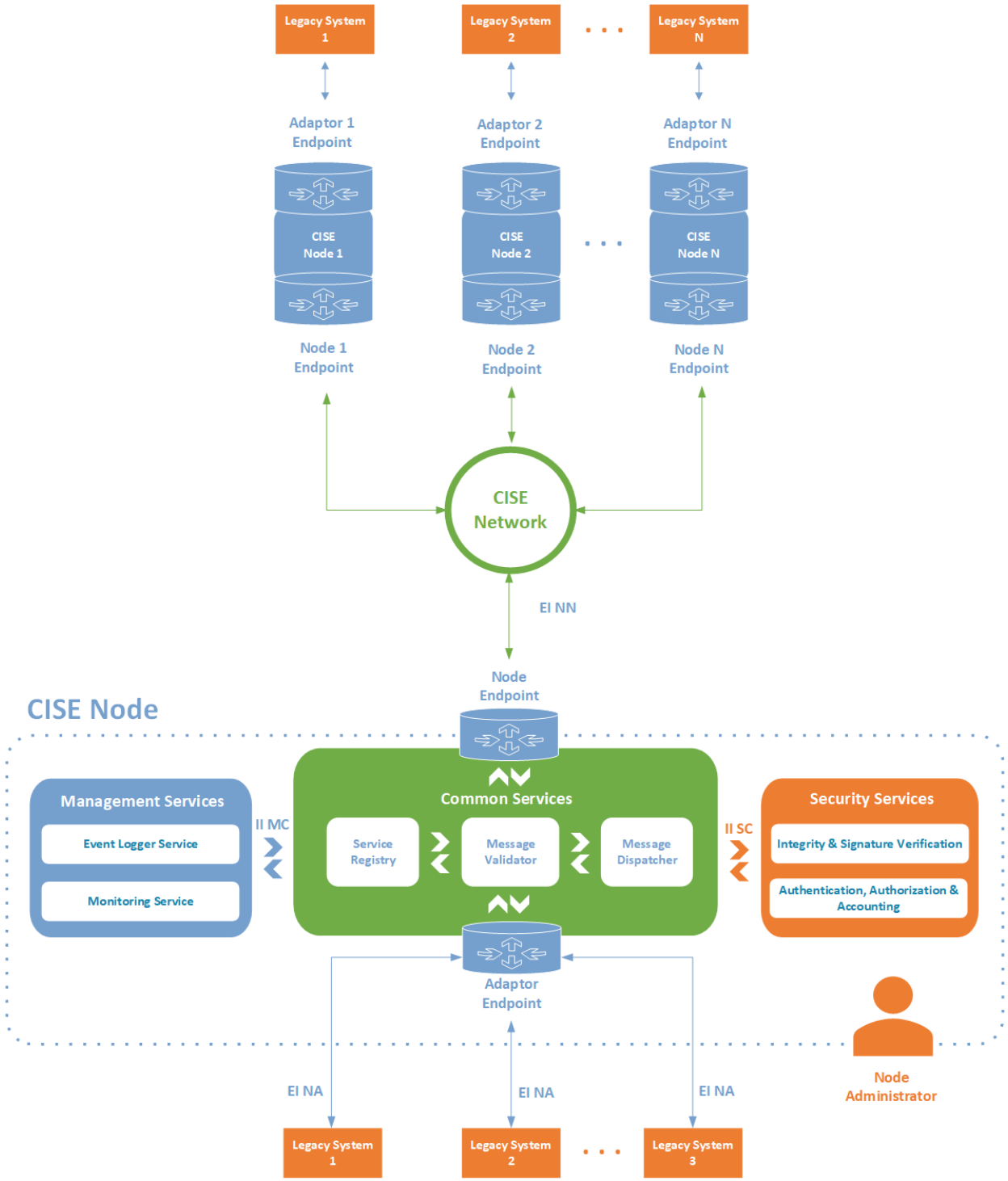


Figure 5: CISE Node Architecture

The CISE Node is organized in three service layers, labelled as in Figure 5, taking care of Common, Management and Security services. Each block is designed to match the normative system-level specifications labelled as core or extended (if only applicable to a specific sector as in the case of the maritime domain): [Fun-Arc-02], [Fun-Arc-03], [Fun-Arc-04] defined in clause 5.1, [Fun-IAA-05] defined in clause 5.2.4, [Fun-NC-01], [Fun-NC-02], [Fun-NC-03] defined in clause 5.2.2 and [Fun-MR-01], [Fun-MR-02], [Fun-MR-03], [Fun-MR-04], [Fun-MR-05], [Fun-MR-06] defined in clause 5.2.3 of ETSI GS CDM 002 [1].

The following interfaces shall be available:

- External Interface Node: Adaptor (EI NA): the interface between the Node and the Adaptor;
- External Interface Node: Node (EI NN): the interface between two nodes in the CISE Network;
- Internal Interface Management services: Common services (II MC): generic interface enabling information exchange between Management and Common services;
- Internal Interface Security services: Common services (II SC): generic interface enabling information exchange between Security and Common services.

In addition, the following requirements shall be applied:

[Gen-REQ-01] The CISE network shall be designed as a global peer-to-peer network without any central component managing the communications between nodes. Both CISE nodes and adaptors are connected via the Internet and fulfil the specifications defined in ETSI GS CDM 002 [1], clause 5.2.2.

[Gen-REQ-02] If Node X wants to communicate with Node Y, a separate VPN-tunnel from X to Y shall be established (see Annex A).

[Gen-REQ-03] Rather than setting up VPN connections on every computer or server providing the services, the connection between the different sites shall be handled by routers/firewalls, one at each location (site-to-site VPN, see Annex A).

In the clauses below the specifications of the functional blocks are detailed.

5.2.2 CISE Node Common Services

5.2.2.0 Overview

When a message enters into a CISE node it passes from a set of elaboration stages. The Common Services undertake the following functionalities:

- provision of a set of RESTful APIs through an endpoint;
- validation / rejection of a message;
- service discovery;
- message dispatching.

5.2.2.1 Node and Adaptor Endpoints

The requests coming from Adaptors and other CISE Nodes will follow the Service Model, as described in ETSI GS CDM 004 [2], and will reach this normative endpoint address. For the API endpoint the following requirements apply:

[Com-NAE-01] All resource URIs of this API shall have the following root:

{apiRoot}/{apiName}/{apiVersion}/endpoint_url

The "apiRoot" and "apiName" are discovered using the service registry (see clause 5.2.2.3). The "apiName" shall be set to "cise" and "apiVersion" shall be set to "v2" for the present document. All resource URIs in the clauses below are defined relative to the above root URI.

[Com-NAE-02] The APIs shall support HTTP over TLS (also known as HTTPS) using TLS version 1.2 (as defined by IETF RFC 5246 [4]). TLS 1.3 (including the new specific requirements for TLS 1.2 implementations) defined by IETF RFC 8446 [5] should be supported. HTTP without TLS shall not be used. Versions of TLS earlier than 1.2 shall neither be supported nor used. COM-NAE-01 requirement illustrates the resource URI structure of this API.

[Com-NAE-03] The APIs are exposed to the local adaptors via the RESTful interface labelled as EI NA.

[Com-NAE-04] The APIs are exposed to other nodes in the CISE network via the RESTful interface labelled as EI NN.

[Com-NAE-05] Messages requesting resources that are not available will trigger an HTTPS error as described in IETF RFC 2660 [6].

5.2.2.2 Message Validator

The Message Validator receives the CISE messages from external nodes via the EI NN or from the adaptors via the EI NA endpoints according to the Service Model described in ETSI GS CDM 004 [2].

It shall therefore comply with the following specifications:

[Com-VAL-01] Accept messages from other CISE Nodes and adaptors through the EI NN or EI NA interfaces;

[Com-VAL-02] Validate messages from syntax and semantics perspectives using the cise-models library to marshal/unmarshal them (CISE message compliant to XML schemes of the CISE Service Model, described in ETSI GS CDM 004 [2]).

[Com-VAL-03] Verify the signature of the messages through the II SC on the basis of the cise-signature library.

[Com-VAL-04] Route the result of the validation and verification actions to the Accounting Service described in clause 5.2.4.1 through the II MC.

5.2.2.3 Service Registry

CISE Nodes are expected to know which services are provided by the CISE Adaptors and by other trusted CISE Nodes connected via the network. They rely on a local registry whose specifications are listed below.

[Com-REG-01] Each CISE Node shall have its own service registry with its metadata. The service registry of each CISE Node shall store in its database a copy of the metadata of other nodes. The Node shall keep updated Table 1.

Table 1: Service Registry Table

Resource name	Resource description
Service ID	Unique identifier of a service in CISE following an agreed scheme (URN), e.g. eu.node_name.authority.vesselService123.
Service Status	• Online. • Offline. • Draft. • Maintenance. • Deprecated.
Service Type	Main data entity exchanged using this service. For instance, a service of type VesselService exchanges vessel data.
Service Operation	Operation supported by the service according to the communication patterns. Possible values: Pull, Push Subscribe, Feedback.
Service Role	Role of the service in the information exchange protocol. Possible values: Consumer, Provider.
Service Profile	Metadata describing the features of the information provided by the service: • Origin (sea basin). • Data freshness (real-time, historical, etc.).
Service Capabilities	Metadata describing the capabilities of the service: • subscription capabilities; • maximum number of concurrent connections; • maximum delay time to receive a reply.
Service Provider	ID of the Legacy System that offers the service.
Service Subscriber List	ID of the consumer services subscribed to the service.

Table 2: HTTPS methods for Service Registry

Resource name	Resource URI	HTTPS method	Description
CISE node capability information	{apiRoot}/{apiName}/{apiVersion}/endpoint_url	GET	Instance to retrieve the CISE Node capability information (Service ID, Service Type, Service Operation, Service Role, Service Capabilities, Service Provider, Service Subscriber List).
CISE node capability information.	{apiRoot}/{apiName}/{apiVersion}/endpoint_url	POST	Instance to create a ServiceID (Service ID, Service Type, Service Operation, Service Role, Service Capabilities, Service Provider).
CISE node capability information	{apiRoot}/{apiName}/{apiVersion}/endpoint_url	DELETE	Instance to remove a ServiceID.

[Com-REG-02] The users of each node can only consult the local copies of the remote nodes metadata, without being able to modify them.

[Com-REG-03] In order to share their metadata, all CISE Nodes shall support a synchronization mechanism by implementing it in the service registry component.

[Com-REG-04] The synchronization mechanism shall support "PULL all remote metadata changes" mechanism, executed at scheduled intervals.

[Com-REG-05] The synchronization mechanism shall support "PUSH existing local services changes" mechanism, executed upon any modification on the local services.

[Com-REG-06] A timeout-based mechanism shall be defined for nodes to respond to the synchronization request. In case a CISE Node responds with a known/unknown error, the other CISE Node shall consider the synchronization attempt as failed and shall be able to trigger again the process after a configured time interval.

[Com-REG-07] The rows in the service registry shall be appended/deleted making use of the POST/DELETE HTTPS methods described in Table 2. The requests are validated through the II MC and the functionality considered in Mgt-MON-02.

[Com-REG-08] The CISE node shall support a discovery mechanism that provides information about: Service Name, Node UUID, Service Profile, Service Capability, Subscription Capability (if the pattern is publish/subscribe). This service can be implemented on the basis of the "GET" method in Table 2.

[Com- REG-09] In presence of an operation of PullRequest SUBSCRIBE/UNSUBSCRIBE, the CISE Node is requested to update Service Subscriber List accordingly.

5.2.2.4 Message Dispatcher

The Message Validator routes the message to the Message Dispatcher. This functional block shall comply with the following specifications:

[Com-DIS-01] The CISE Node supports the operations listed in Table 3 through the Node and Adaptor endpoints, described in clause 5.2.3.1.

[Com-DIS-02] Separate the messages to be routed to adaptors connected to the node from the ones that need to be addressed to other nodes. By checking the information available in service registry, it shall be possible to discover if the Adaptor is local or remote.

[Com-DIS-03] In presence of messages addressed to Adaptors (as from the recipient adaptor url specified in the message (**participant/endpointUrl** tag):

- Deliver the message to the recipient adaptor.
- Send async-ack to inform the sender that the message has been delivered to the destination (only if the required ack is present).

Table 3: HTTPS methods on Node Services

Resource name	Resource URI	HTTPS method	Meaning	Parameters	Return Value
CISE node service	{apiRoot}/{apiName}/{apiVersion}/ endpoint_url	PULL	This operation is used to request information using a query-by- example mechanism.	Data template (including the main entity of the service). Capabilities requested.	A list of [Main Entity] + [Entities directly related to the main one]. Capabilities offered.
CISE node service	{apiRoot}/{apiName}/{apiVersion}/endpoint_url	PUSH	This operation is used to push information to a CISE consumer. The origin of the notification might be a previous subscription.	A list of [Main Entity] + [Entities directly related to the main one]. Capabilities offered.	Acknowledgement
CISE node service	{apiRoot}/{apiName}/{apiVersion}/endpoint_url	SUBSCRIBE	This operation is used to subscribe or unsubscribe to a series of notifications on specific information.	Data template (including the main entity of the service). Capabilities requested.	Acknowledgement Capabilities offered
CISE node service	{apiRoot}/{apiName}/{apiVersion}/endpoint_url	FEEDBACK	This operation is used to provide feedback on information already exchanged.	Reference to the previous exchange. Nature of the issue.	Acknowledgement

[Com-DIS-04] In presence of messages addressed to other nodes (as from the recipient node url specified in the message (**gateway/endpointUrl** tag):

- Deliver the message to the recipient node.
- Send async-ack to inform the sender that the message has been delivered to the destination(only if the required ack is present).

5.2.3 CISE Node Management Services

5.2.3.1 Monitoring Service

This functional block shall be managed by the Node Administrator through an interface and shall allow to keep track of all events occurring in Common Services.

[Mgt-MON-01] Provide the overall status of the node in terms of the services listed in the Service Registry (see clause 5.2.2.3) by marking the status of the services as online, test, maintenance and deprecated.

[Mgt-MON-02] Fulfil the incoming requests of service creation and deletion.

[Mgt-MON-03] Manage the change of status of each service.

5.2.3.2 Event Logger Service

This functional block shall:

[Mgt-LOG-01] Keep trace (for instance making use of a database) of the events routed by the Message Validator and Message Dispatcher through the II MC.

The logger service shall save the minimum set of logging information described in Table 4.

Table 4: Logger of events

operation_id	Operation Unique Identifier.
event_type	Event name.
log_message	Outcome of validation and verification. Concatenation of verification and validation results.
event_creation_date_time	The date of event creation.

The supported events shall include the following types: message events, service events, participant events, node events, user management events, streaming events and security events.

5.2.4 CISE Node Security Services

5.2.4.1 AAA Services

This functional block shall:

[Sec-AAA-01] Provide the System Administrator with all functionalities for user accounting and node management (e.g. management of CISE participants, management of CISE services, management of the Access Right Matrix, management of service subscribers, management of users and roles of the CISE node, management of the certificates for messages signature and validation).

[Sec-AAA-02] Provide an API to authenticate the (human/system) user with defined roles (e.g. super admin, observer, Legacy System owner, etc.).

[Sec-AAA-03] Implement the CISE access control policy. Participants shall be connected to the network and are authorized to access the relevant information and services according to the User Community they belong to, national agreements and operational purpose (Access Right Matrix). If the Consumer has the right to query or to subscribe to a service, the Provider shall return only the information elements allowed by the Access Right Matrix.

Rules shall be defined on the basis of:

- Participant Rules:
  - a set of rules for each Service published in order to define the Participants that may have access or not to it.
- Access Right Matrix Check Flow:
  - when the Participant wants to consume a service provided by another Participant (Pull request), this functional block (part of the AAA block, as depicted in Figure 5) shall reply with a response detailing if the consumer is allowed to retrieve all or only part of the available information.

[Sec-AAA-04] Inform the Common Service block to deliver the message to the Consumer only if proper rights are set up in the Access Right Matrix defined above. The message shall contain only the information allowed in the Access Right Matrix.

5.2.4.2 Signing Service

The message signature mechanism when messaging is done from Adaptor A, connected to CISE Node A, to Adaptor B, connected to CISE Node B, needs the following capabilities:

[Sec-SIG-01] The authentication mechanism used to access CISE network shall be based on X.509 certificates, according to Recommendation ITU-T X-509 [3] issued by Dedicated PKI Certification Authorities as described in Annex C.

[Sec-SIG-02] In case of receiving a signed message from Adaptor A:

- Verifies the signature of Adaptor A;
- Signs the whole message again using the CISE Node A Certificate;
- Sends the message to the recipient CISE Node B.

[Sec-SIG-03] In case of receiving a signed message from CISE Node A, originated by Adaptor A:

- Verifies the signature of CISE Node A;
- Signs the whole message again using CISE Node B Certificate trusted by Adaptor A;
- Sends the message to the recipient Adaptor B.

[Sec-SIG-04] In case of receiving a signed message from CISE Node B:

- Verifies the signature of the message from CISE Node B;
- Processes the whole message.

Figure 6 shows the message life cycle between Adaptor A and Adaptor B.

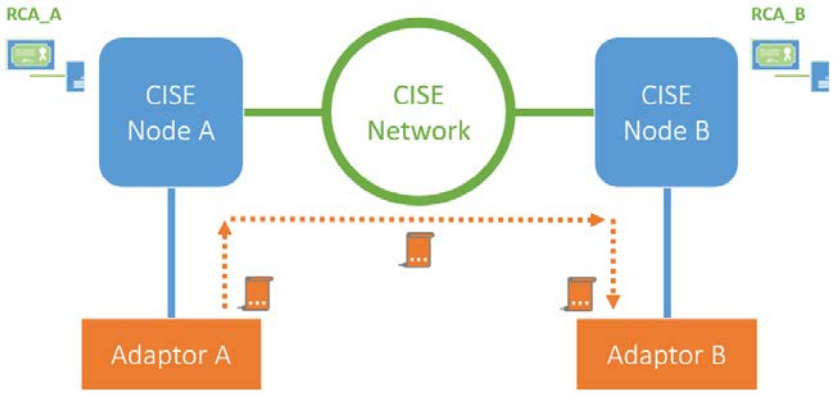


Figure 6: message life cycle between Adaptor A and Adaptor B

[Sec-SIG-05] Both CISE Nodes and Adaptors shall include the following additional capabilities while performing signature validation mechanism:

- Providing a success acknowledgement to the sender when a signed message is received.
- Providing an invalid signature acknowledgement to the sender when a message with a corrupted signature is received.
- Providing an invalided signature acknowledgement to the sender when a message with a corrupted certificate is received.
- Providing an invalid signature acknowledgement to the sender when a message with corrupted digest is received.
- Providing an invalid signature acknowledgement to the sender when a message with an unsupported signature algorithm is received.
- Providing an invalid signature acknowledgement to the sender when a message with an unsupported digest signature algorithm is received.

5.3 Performance

Performance requirements shall be compliant with clause 6 of ETSI GS CDM 002 [1]. No specific performances are requested at the architecture level.

Annex A (informative): VPN security configurations (Unclassified network)

A.1 Introduction

The present annex describes the solution elements which are proposed to support the communications among the CISE Nodes and the Legacy Systems.

The network is designed as a global peer-2-peer network without any central component managing the communications between nodes. A private virtual network is established between nodes using public Internet as communication transport media and using IPSEC protocol for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session using cryptographic keys.

Within the virtual network, there is no routing. If Node A wants to communicate with Node B, a separate VPN-tunnel from A to B will be established.

Rather than setting up VPN connections on every computer or server providing the services, the connection between the different sites will be handled by routers/firewalls, one at each location (Site-to-site VPN).

Once configured, the routers/firewalls will maintain a constant tunnel between them that links the different sites. In this scenario, users do not have to do anything to initiate the VPN session because it will be always on (see Figure A.1).

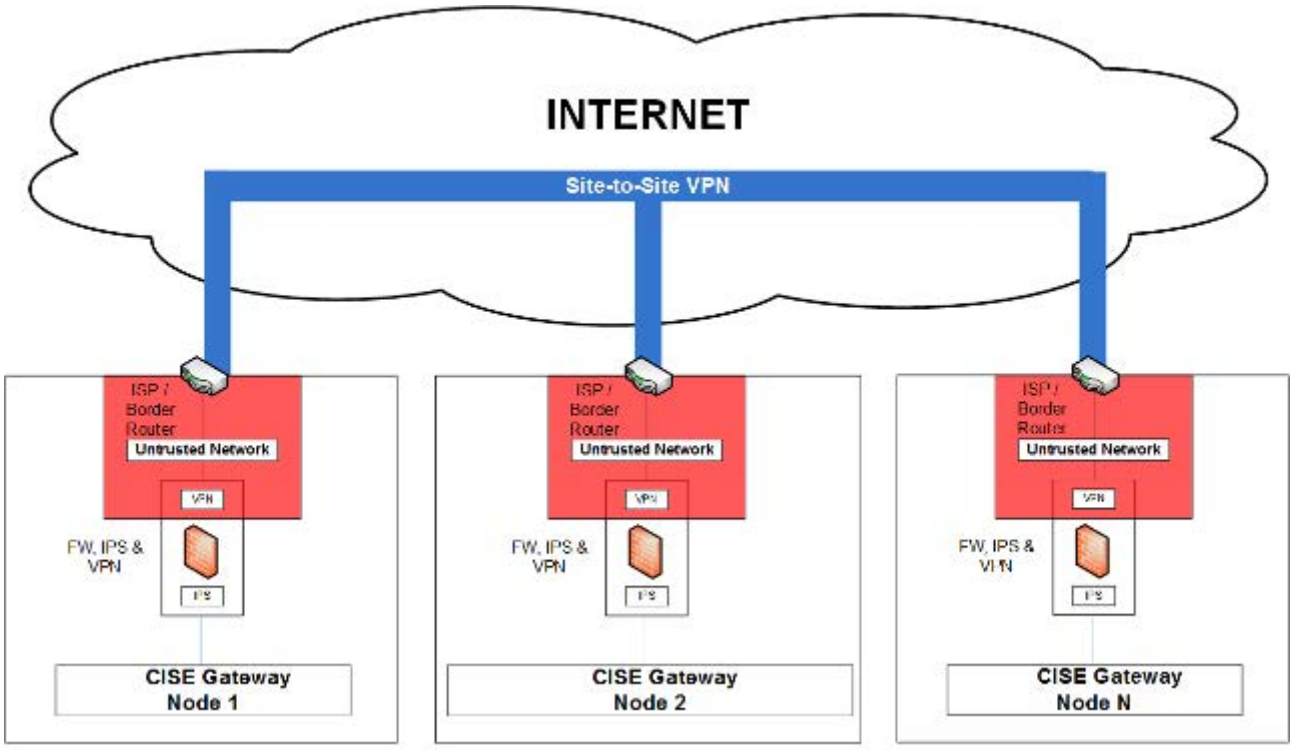


Figure A.1: CISE Site-to-Site VPN's concept

Annex B (normative): CISE topology

There are different ways Public Authorities can connect to the CISE Network:

1) Public Authority directly connected to CISE with its own Node (see Figure B.1).

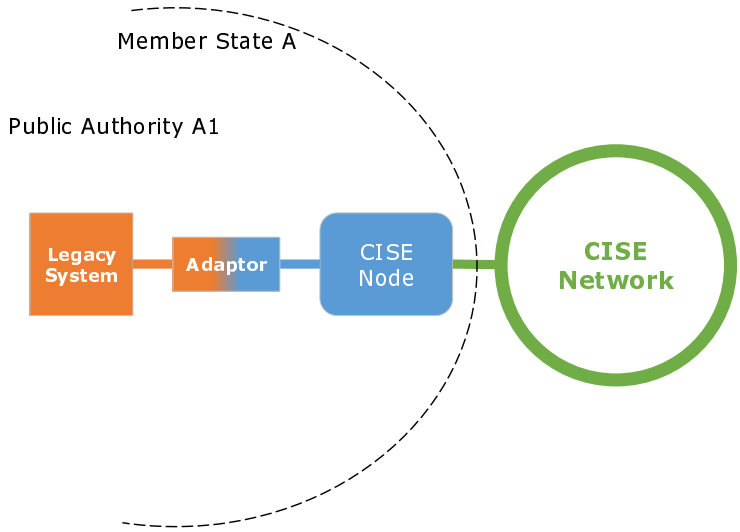


Figure B.1: Public Authority directly connected to CISE with its own Node

2) More than one Public Authority connected to CISE with one shared Node and one or more legacy systems (see Figure B.2):

   - The Node shall handle the routing between all Legacy systems connected to the Node via different Adaptors. Legacy systems may belong to the same Public Authority or different Public Authorities.

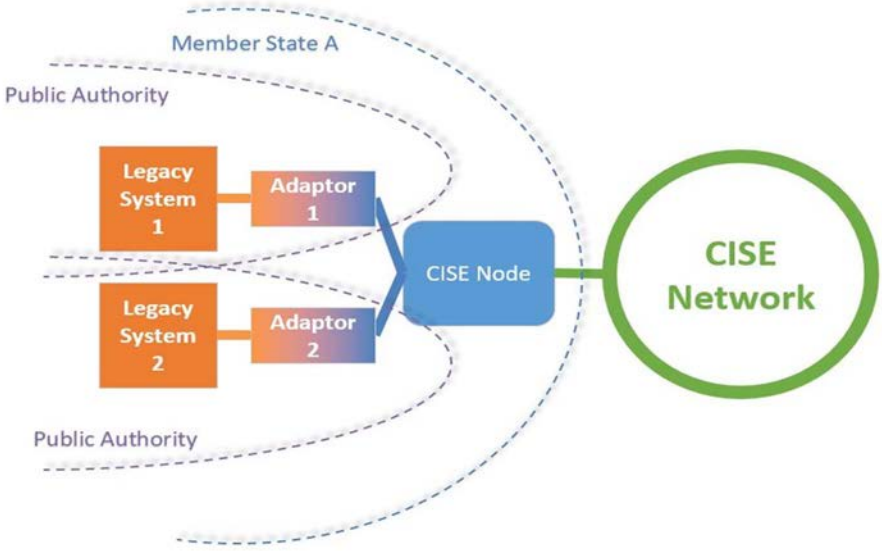


Figure B.2: Public Authorities connected to CISE with a CISE Node

3) Public authorities connected through a National Information System (see Figure B.3):

   - The National Node shall handle the proper redistribution of data among the Legacy Systems.
   - The Node shall give access to the National Information System.

- The National Information System shall be connected to the CISE Node with one single Adaptor.

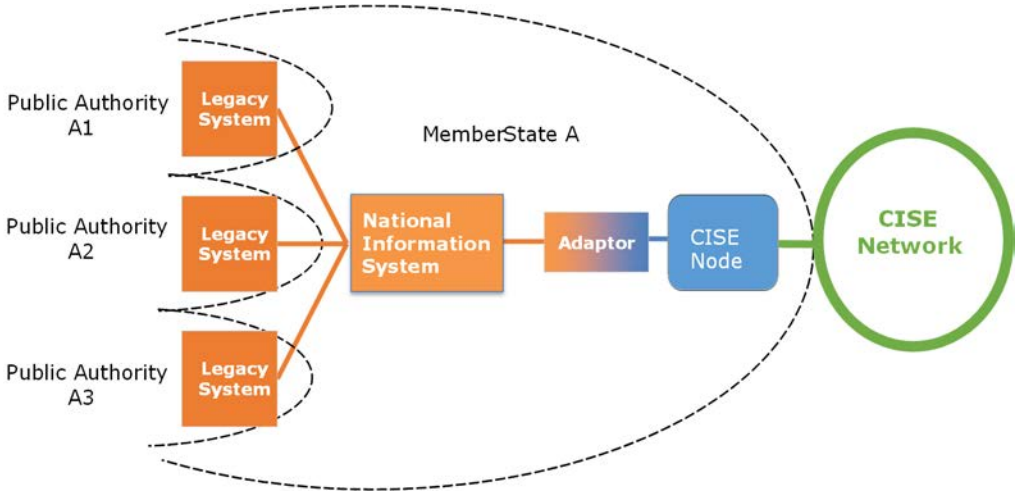


Figure B.3: Public authorities connected through a National Information System

4) Public authorities connected through a Regional Information System (see Figure B.4):

- The Regional Information System shall be connected to the CISE Node with one single Adaptor.

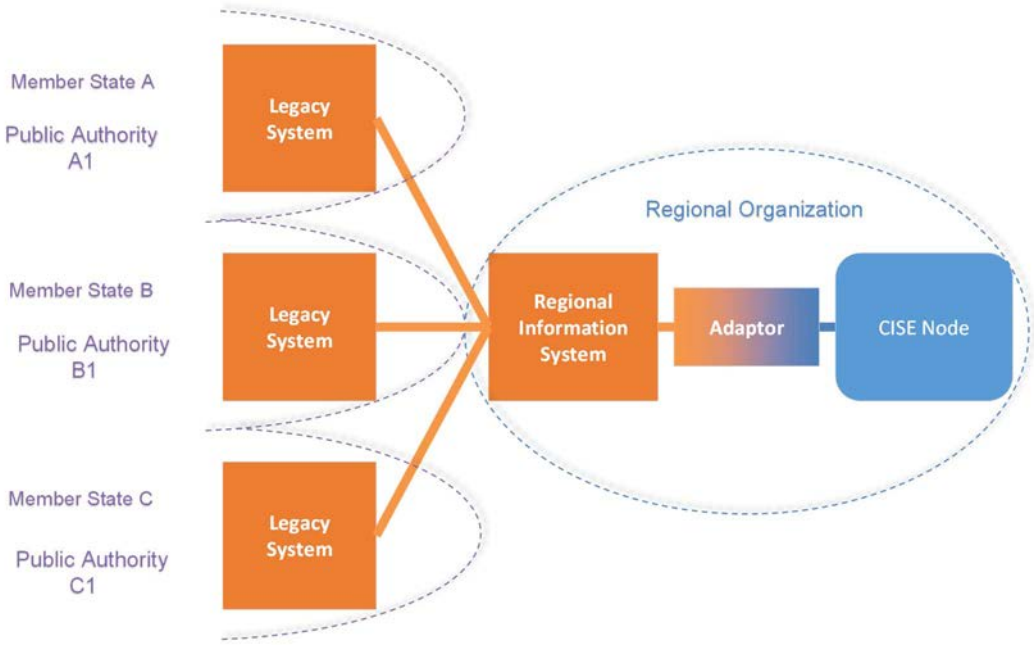


Figure B.4: Public authorities connected through a Regional Information System

CISE is a Public Information Sharing Environment as it manages information that can be accessed by a Sector and it shall not affect the functionalities of the operational information systems belonging to the participating Public Authorities or of the European existing sectorial information systems.

Figure B.5 shows the end-to-end vision, reporting all the previously described configurations.

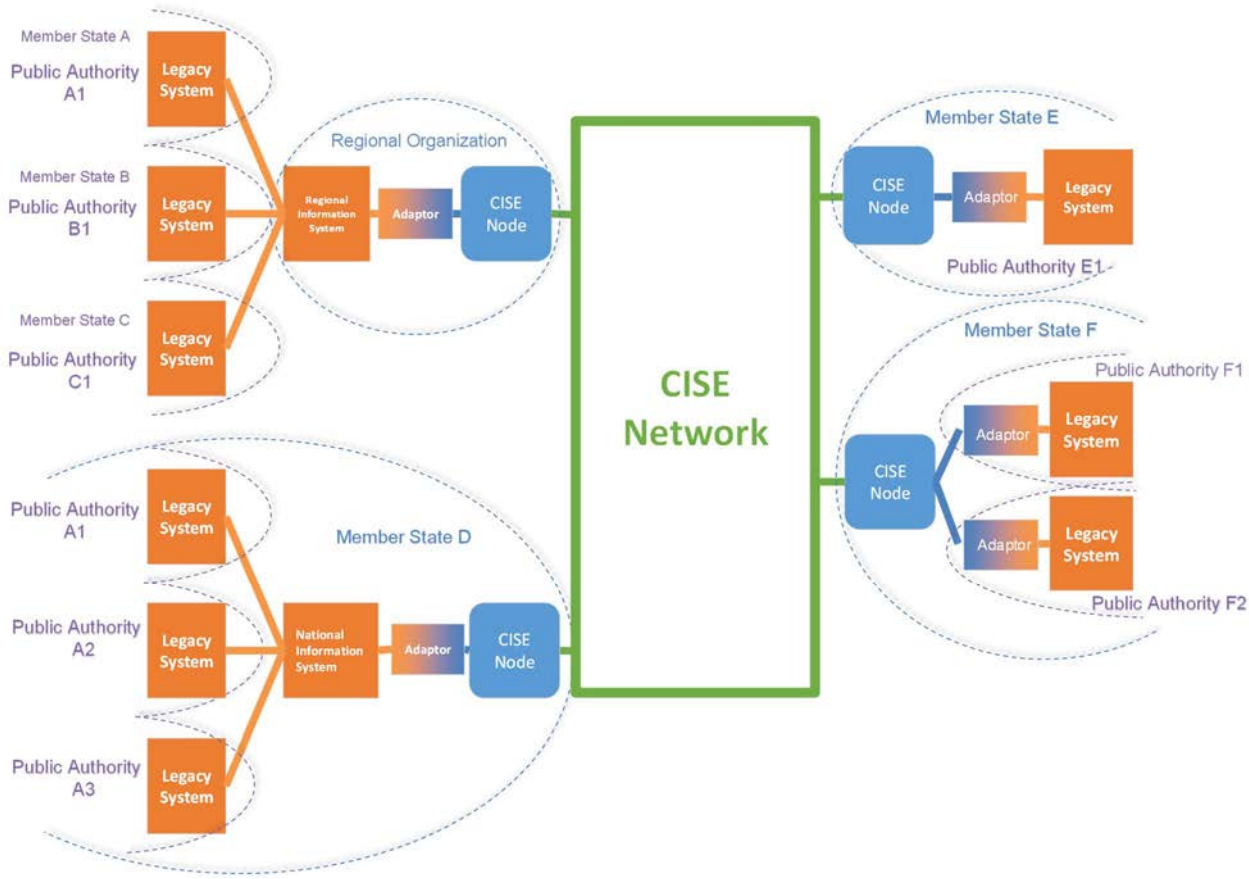


Figure B.5: End-to-end vision

Annex C (informative): The CISE PKI

The normative provisions are discussed in clause 5.2.4. Hereby it is reported the recommended configuration of the PKI governing the CISE network.

A Root Certification Authority is implemented at the global CISE scope while local Certification Authorities are hosted in every Node. This mean that a CISE user, linked to a given Node, and hence trusted by its own Certification Authority, can request data and services on all the other CISE Nodes.

Every Member State owns its PKI recognized by the Root CA. Any CISE Node trusts the Certification Authority of all other CISE Nodes relying on the Root CA.

The data integrity and user authentication can be ensured by using the XML signature, which is encapsulated in every message exchanged via CISE Nodes.

Annex D (informative): Change history

Date	Version	Information about changes
May 2021	V1.1.1	First version
June 2024	V2.1.1	New schema of the architecture introduced, applicable to other vertical domains (including land border). Specifications alignment based on the transitional phase led by EMSA. Introduced requirements related to the synchronization mechanism for the service registry. Updated Annex C with the proper architecture used for the implementation of the CISE PKI.

History

Document history		
V1.1.1	May 2021	Publication
V1.2.1	July 2024	Publication
V2.1.1	August 2024	Publication