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

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

Disclaimer

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

Reference
DGS/CDM-003

Keywords
architecture, data models, maritime

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

On October 2009 the European Commission adopted a Communication "Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain (CISE)", promoting to integrate maritime surveillance activities of all public maritime sectors across Europe.

Figure 1: Schematic diagram of the CISE vision

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

The added value of integrating maritime surveillance is to enhance the present sectoral maritime awareness pictures of the sectoral user communities, with additional relevant cross- sectoral and cross-border surveillance data on a responsibility to share basis. Such enhanced pictures increase Member States authorities' efficiency and improve cost effectiveness.

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

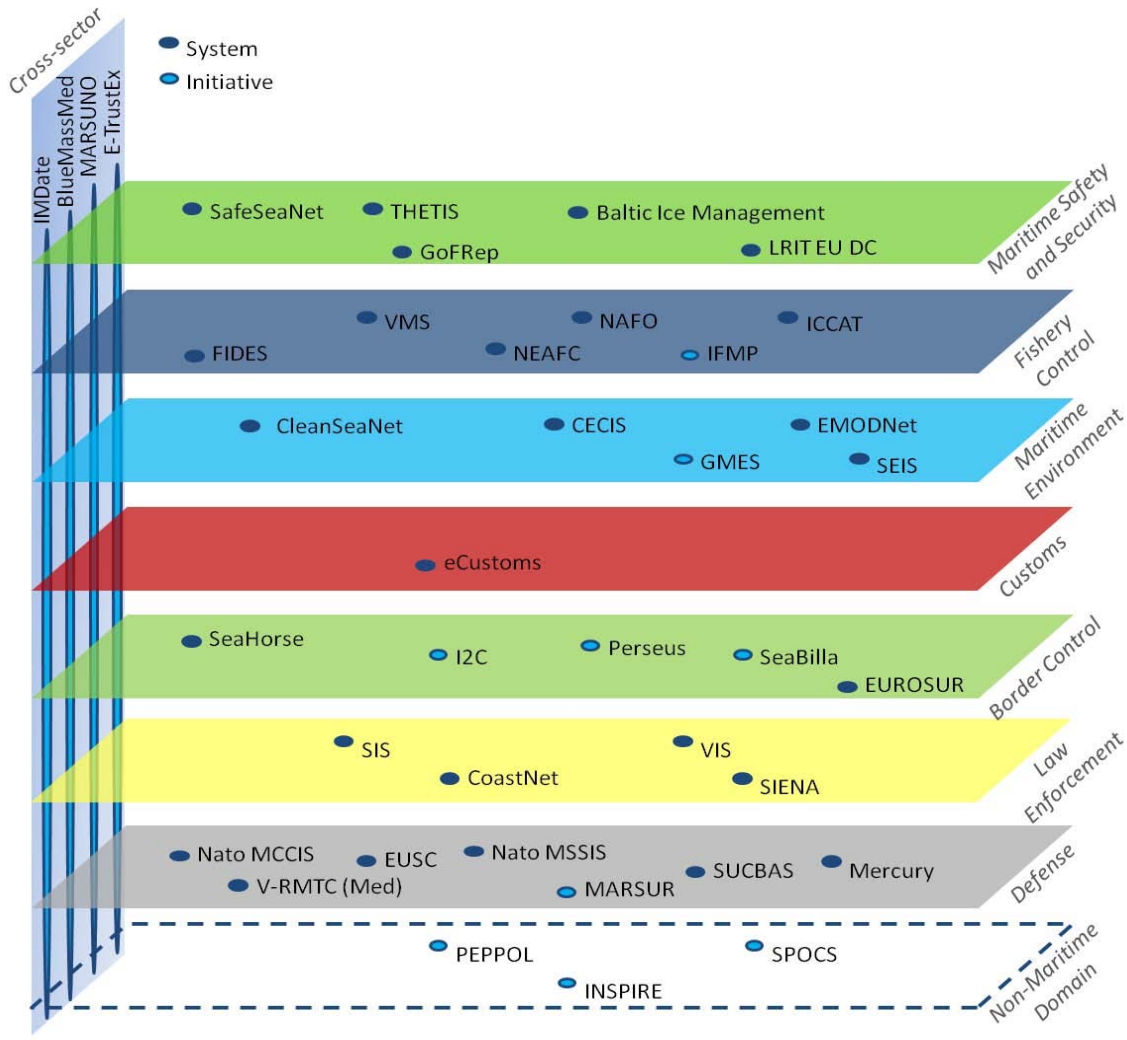

Figure 2: Existing sectoral information systems

To achieve the goals of the CISE vision, a series of EU sponsored projects, building up one on another, further investigated and developed the CISE vision, starting with the elaboration of the so- called CISE principles, which were defined as follows according to CISE Architecture Visions Document [i.2]:

- *"CISE must allow the interlinking of any public authority in the European Union (EU) or European Economic Area (EEA) involved in maritime surveillance".*
- *"CISE must increase maritime awareness based on the "responsibility-to-share" principle".*
- *"CISE must support a decentralised approach at EU-level".*
- *"CISE must provide interoperability between civilian and military information systems".*
- *"CISE must be compatible and provide interoperability between information systems at the European, national, sectoral and regional levels".*
- *"CISE must support the reuse of existing tools, technologies and systems".*
- *"CISE must provide for seamless and secure exchange of any type of information relevant to maritime surveillance".*
- *"CISE must support the change of services by information provider (orchestration)".*
- *"CISE subscribers and stakeholders should be entitled to obtain information only if they also contribute in a way commensurate with their capabilities".*

The CISE roadmap process that started with the definition of the CISE principles is shown in Figure 3:

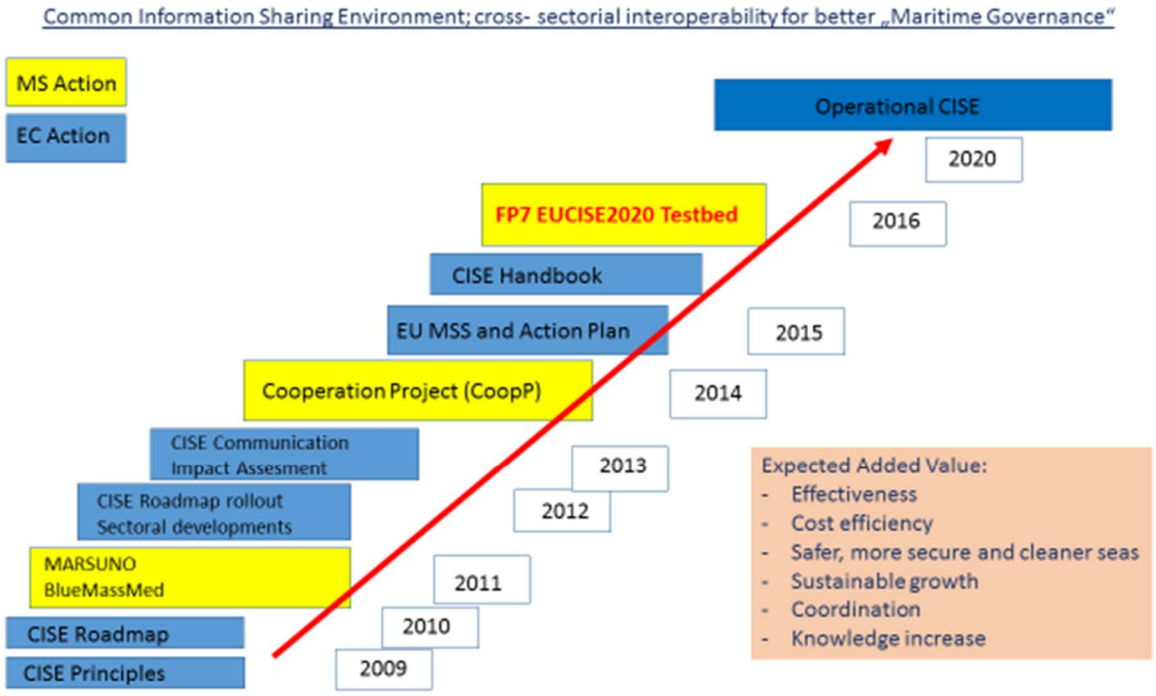

Figure 3: CISE Roadmap

During the roadmap process, a range of 82 use cases was defined representing the entire range of activities of the 7 maritime sectors and their related Coast Guard activity. Out of this range of 82 use cases, 9 use cases were identified as most characteristic and comprehensive, covering the most relevant activities of all sectors. These use cases were to form the operational basis for the further and more detailed investigation of CISE cross- sectoral and cross border information exchange.

The pre- operational validation project **"European test bed for the maritime Common Information Sharing Environment in the 2020 perspective", in short "EUCISE2020"**, based on the 9 use cases selected, defined the requirements for and developed the common architecture of the CISE information exchange network. Consequently, a total of 11 so- called "CISE Nodes" were built, integrated and successfully tested in 8 European countries, connecting a total of 20 sectoral legacy systems of various nature.

Figure 4: Diagram of the EUCISE2020 testbed set-up

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

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

1 Scope

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

The present document describes the following architecture:

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

2 References

2.1 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR CDM 001 (V1.1.1): "Common Information Sharing Environment Service and Data Model (CDM); Use Cases definition".

[i.2] CISE Architecture Visions Document, Version 3.00, 06/11/2013.

NOTE: Available at https://webgate.ec.europa.eu/maritimeforum/en/node/4039.

[i.3] Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU).

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

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

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

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

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

activity: activity performed by a sector

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

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

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

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

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

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

consumer: participant requesting Services over CISE network, only consuming but not providing information

CoopP: project financed by the European Commission in 2013 defining the CISE use cases and the first version of the CISE data and service model

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

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

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

EUCISE2020: FP7 pre-operation validation project on CISE

NOTE 1: The project defined and developed the existing CISE Network and software (2014-2019).

NOTE 2: More information on the project can be found at http://www.eucise2020.eu/.

EU RESTRICTED: classified information covered by the definition of EU security classification levels.

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

NOTE 2: The following EU security classification levels are defined:

- EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.
- EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

- EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.
- EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

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

Legacy System (LS): software designed to perform specific tasks and that exposes certain functionalities through interfaces in the domain of the maritime surveillance

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

message: One of the structured sentences exchanged between Participants to discover, request and provide Services.

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

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

node administrator: role assumed by a User to manage the CISE Node software, hardware and network connections.

node configuration manager: role assumed by a User to manage the declaration of services in the CISE network.

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

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

provider: participant providing Services over CISE network

public authority: any organisation or legal entity that has an interest in maritime surveillance information

NOTE 1: An authority can be local, regional, national or European.

NOTE 2: This organisation may have responsibilities linked to one of the seven sectors of maritime surveillance.

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

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

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

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

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

sector: user community involved in maritime surveillance

NOTE: The seven sectors are the following:

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

- Defence

sea basin: sea area

NOTE: The following sea areas are identified:

- Atlantic
- Baltic Sea
- North Sea
- Mediterranean
- Black Sea
- Outermost Regions
- Arctic Ocean

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

site: physical place where CISE Node is deployed

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

state-of-the art security configuration: most recent stage in security measures implemented to reduce cyber vulnerabilities

unclassified: information to which access is not restricted by law or regulation

user: person appointed by the public authorities, interacting directly with CISE or with a Legacy System connected to CISE

3.2 Symbols

Void.

3.3 Abbreviations

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

AH	Address Hashing
CA	Certification Authority
CAA	Crypto Approval Authority
CDM	CISE Data Model
CISE	Common Information Sharing Environment
CT	Collaboration Tools
DH	Diffie Hellman
DM	Data Model
DNS	Domain Name Server
EEA	European Economic Area
EU	European Union
EUCISE2020	European Union Common Information Sharing Environment
FTP	File Transport Protocol
GW	Gateway
HTTP	Hypertext Transfer Protocol
IAA	Identification, Authentication and Authorization

IKE	Internet Key Exchange
IM	Instant Mesasaging
IP	Internet Protocol
IPSEC	Internet Protocol SECurity
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JSON	Java Script Object Rotation
LS	Legacy System
MR	Message Routing
MS	Member State
NC	Not Classified
PKI	Public Key Infrastructure
REST	Representational State Transfer
RTP	Real Time-Transport Protocol
SFTP	Secure File Tranfer Protocol
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URI	Uniform Research Indentifier
VPN	Virtual Private Network
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

4 Overview

The present document presents the architecture for the information sharing environment identified in CISE Architecture Visions Document [i.2].

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

The network vision concept is that each Member State and Sectors can adopt one of the following paradigms:

- **One-way approach:** all public authorities in a Member State are connected to the CISE network through a single access point.
- **Multi-way approach:** the public authorities of a Member State are connected to the CISE network through different access points.

The CISE environment is designed to allow the interoperability of national or European legacy systems belonging to public authorities in the Member States through two components:

- **CISE Adaptor**, which allows a legacy (LS) system to connect to a CISE Node. It converts the LS data into the common CISE data model.
- **CISE Node**, which implements common CISE specifications and implements CISE messaging protocol for exchange with the CISE adapter or other CISE Nodes.

The services developed in CISE are organized into two classes:

- **Infrastructure (Core Services)**, which represent the basic services implemented by the CISE Node in order to ensure the connection of each partner, or group of them, to the CISE network.
- **Interface (Common Services)**, which are dedicated to the transfer of entities within the CISE network following the CISE rules.

In accordance with the aforementioned, CISE implements the network architecture defined in [i.2] and also shown in Figure 5:

- The CISE national component shall be able to connect to the CISE network one or more public authority of the same Member State. In this configuration, the CISE national component acts as a Gateway (GW) and hosts the Infrastructure and Interface services.

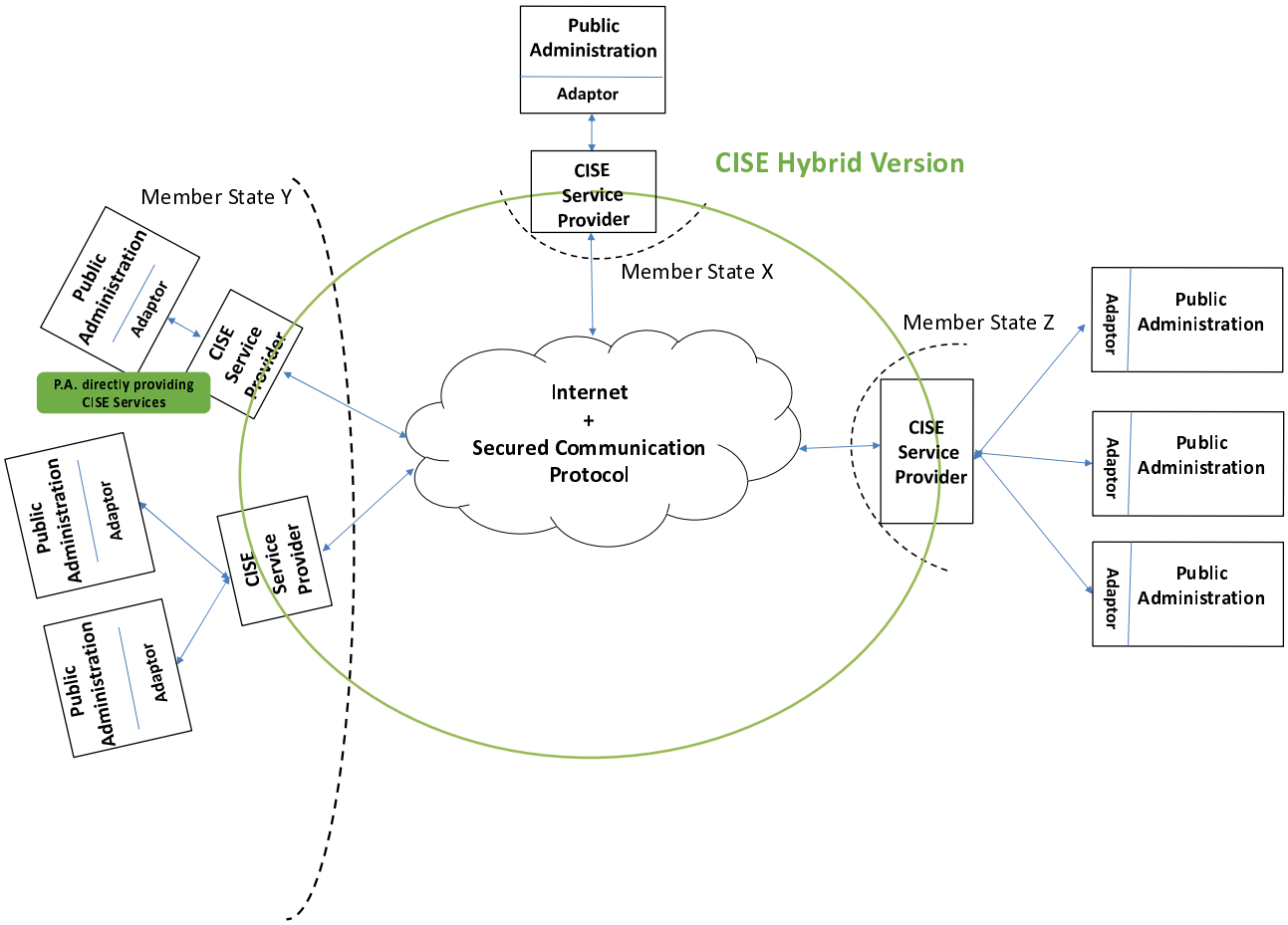

Figure 5: CISE Vision - High Level Operational Concept

5 Architecture description

5.1 High Level Architecture

Clause 5 illustrates the architectural design of the system that has been done by following a gradual decomposition process. Starting from an analysis of the context, the reference architecture model which led the decomposition of the system into software components has been chosen.

The CISE shall allow the Legacy Systems to exchange data.

The Adaptors are the architecture components 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.

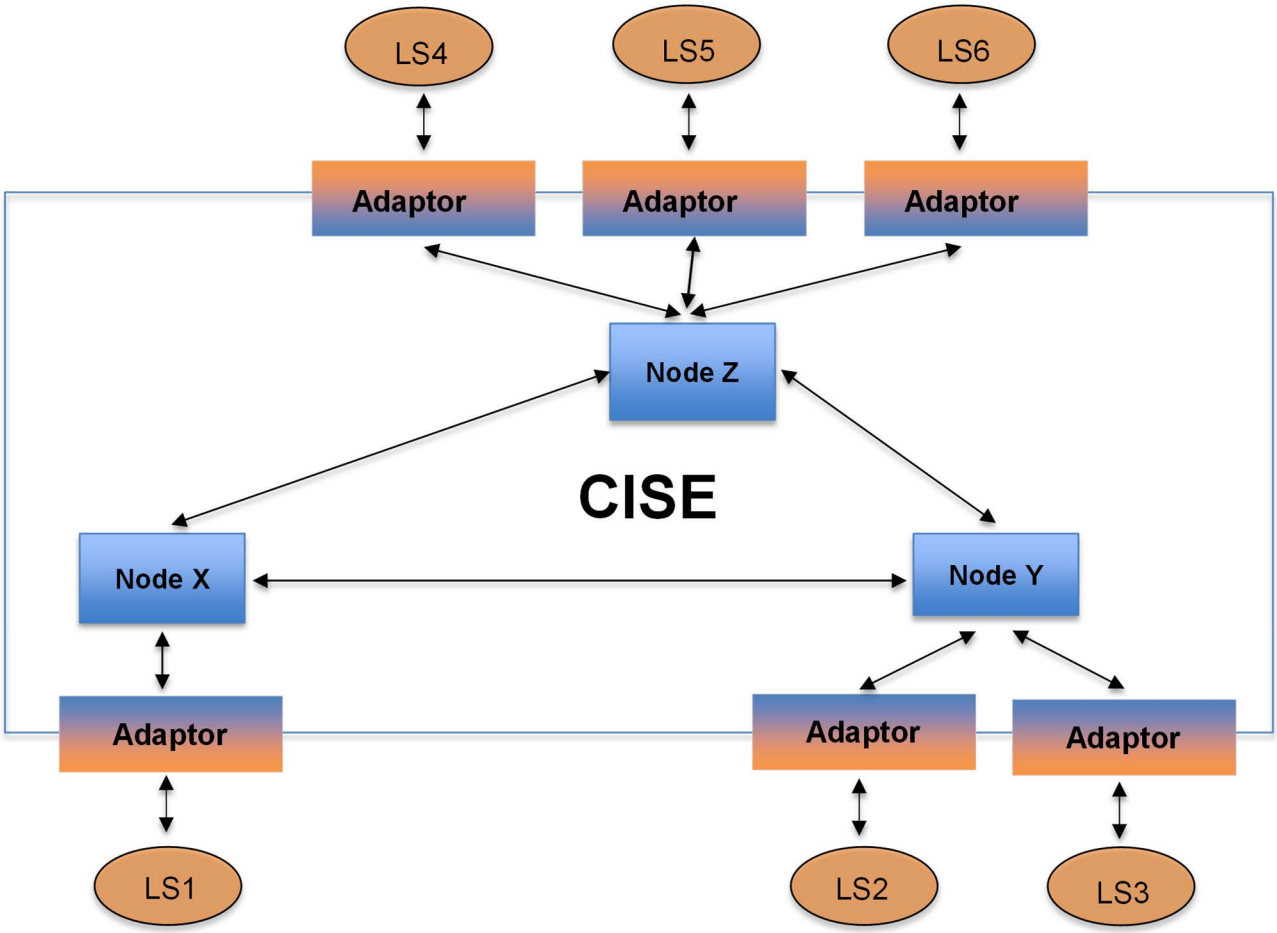

Figure 6: CISE environment

The Adaptor role is to connect seamlessly the Legacy System to the CISE network.

In this environment (see Figure 6), a Legacy System is connected to CISE using one Adaptor for each Legacy System and one CISE Node.

The CISE Architecture defines the way a Legacy System is connected to the CISE Network.

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 7 below):

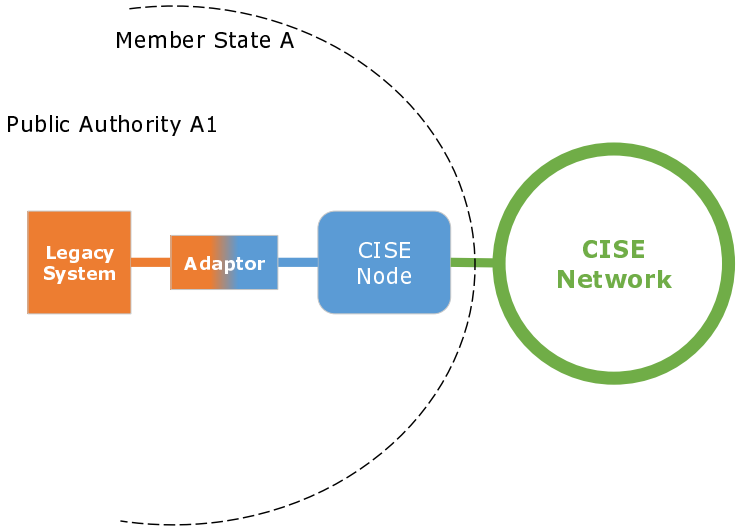

Figure 7: Public Authority directly connected to CISE with its own Node

2) More than one Public Authority connected to CISE with one shared Node and one or more legacy systems (see Figure 8 below):

- 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.

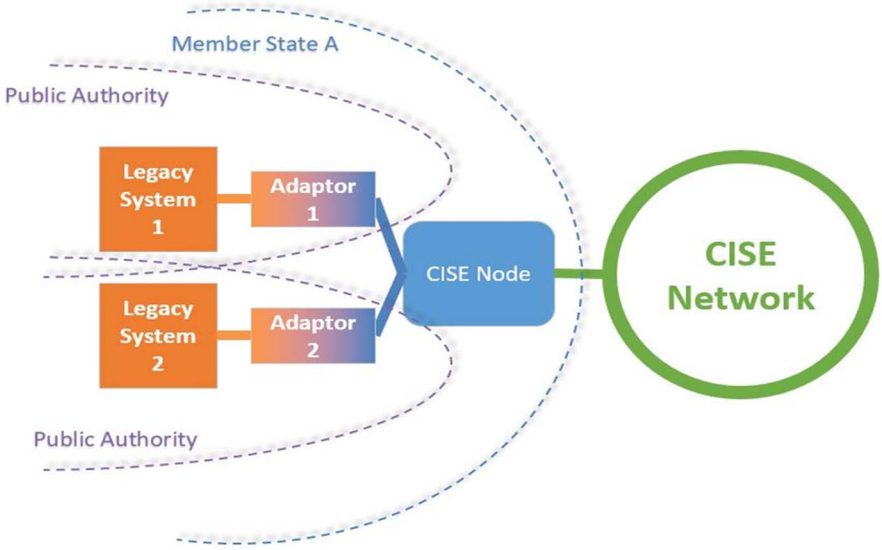

Figure 8: Public Authorities connected to CISE with a CISE Node

3) Public authorities connected through a National Information System (see Figure 9 below):

- 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.

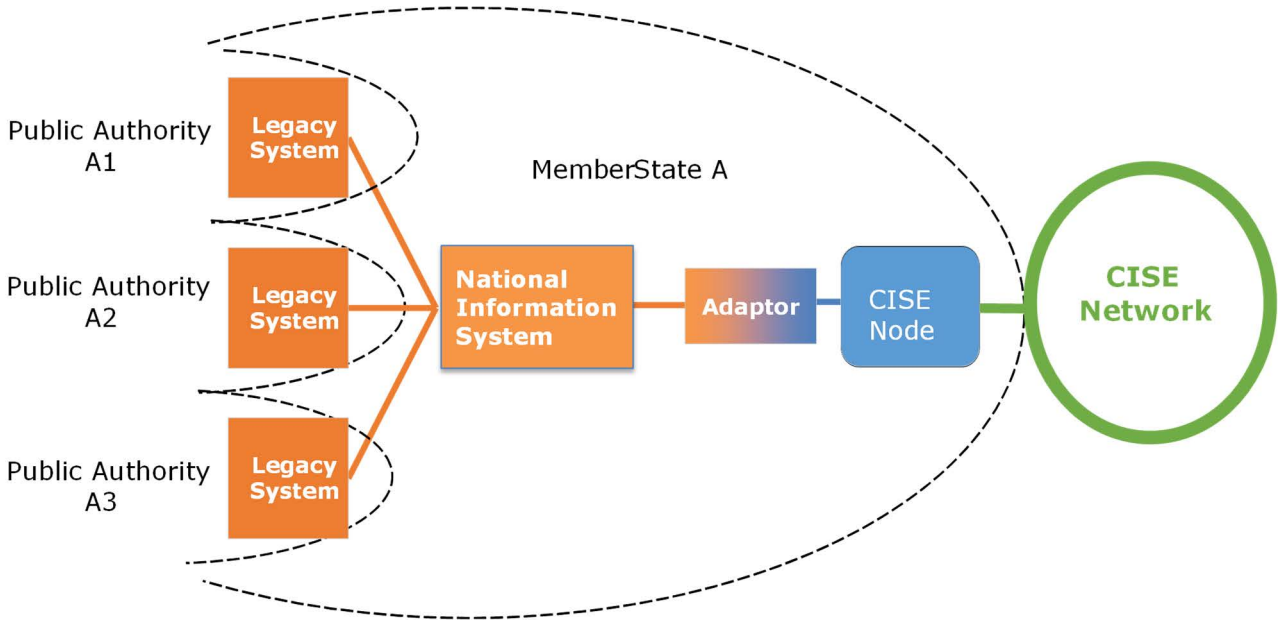

Figure 9: Public authorities connected through a National Information System

4) Public authorities connected through a Regional Information System (see Figure 10 below):

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

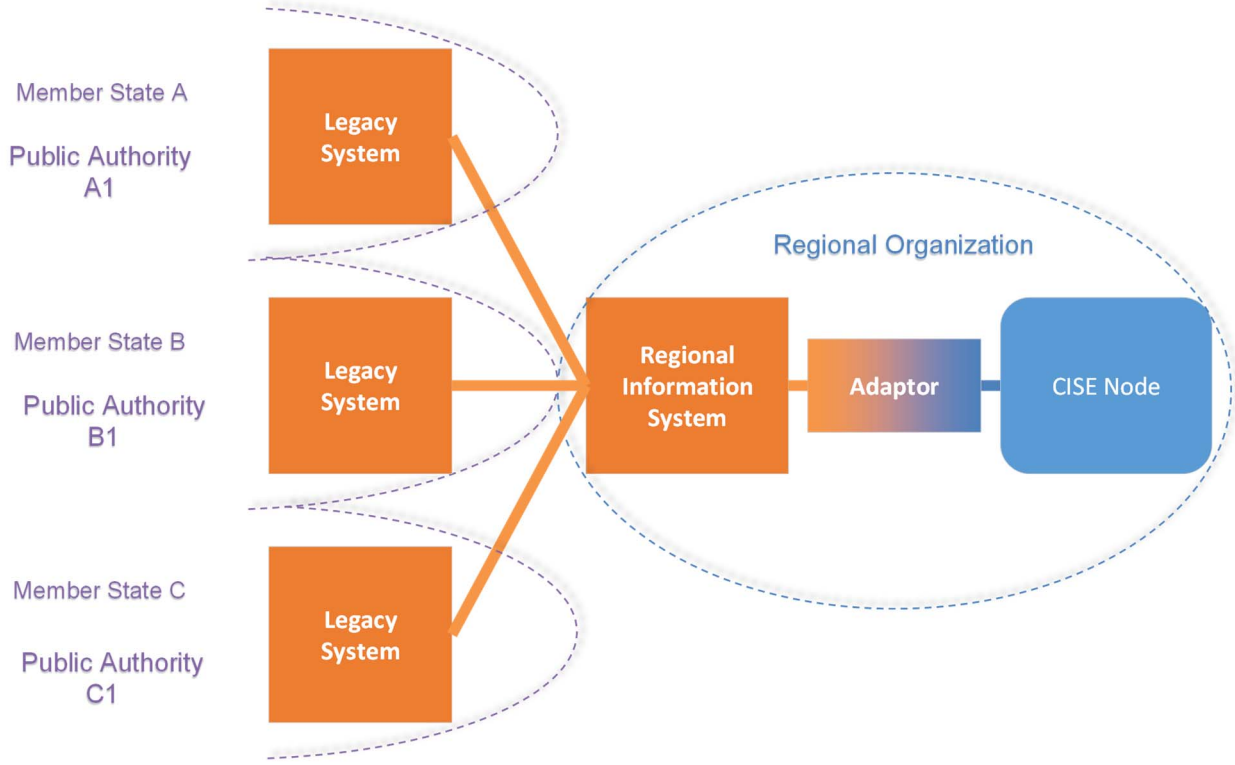

Figure 10: Public authorities connected through a Regional Information System

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 11 shows the end-to-end vision, reporting all the previously described configurations.

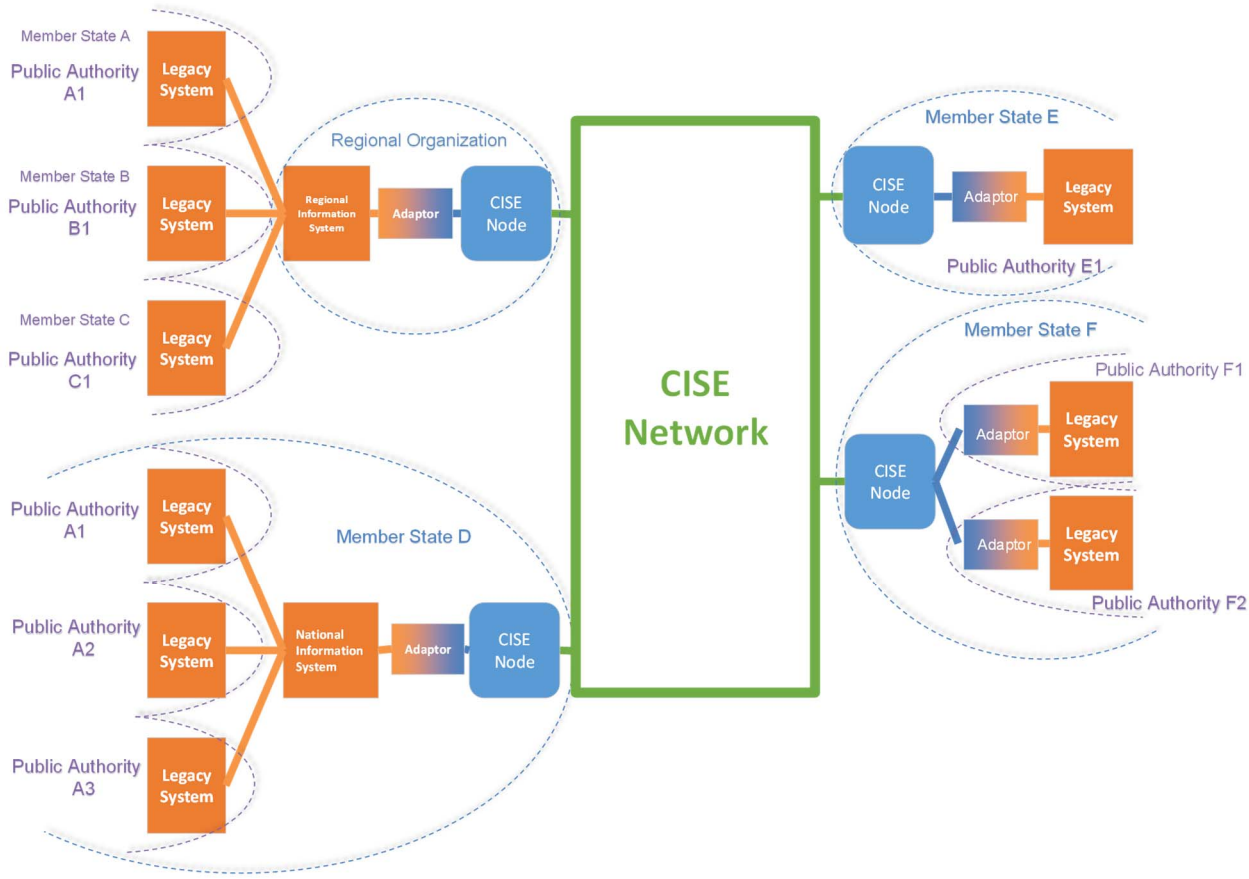

Figure 11: End-to-end vision

5.2 Network Architecture

5.2.1 General Requirements

The network architecture shall implement the requirements [Fun-Arc-02], [Fun-Arc-03], [Fun-Arc-03] 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].

5.2.2 The Adaptor-Node interface

The Adaptor is the bridge between the Legacy System and the Infrastructure Services (available in the Node).

As such, the Adaptor shall have two integrations points towards the Node: the outbound for sending messages and the inbound, for receiving messages.

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

The Node shall support both SOAP and REST protocols for the communication with the Adaptor.

The Interface Services shall be available through a single generic Web Service interface that has a single operation supporting every message exchange pattern as well as every operational service type.

The Adaptor shall implement the CISEMessageService interface needed to communicate with the CISE Node.

The choice to use the SOAP or REST interface is a decision of the Adaptor but shall be set during the service registration in the Node.

NOTE 1: SOAP is XML based protocol that consists of four parts:

- envelope that defines a framework for describing what is in a message and how to process it;
- set of encoding rules for expressing instances of application-defined data types;
- convention for representing remote procedure calls and responses; and
- binding convention for exchanging messages using an underlying protocol.

NOTE 2: REST is a software architectural style that defines a set of constraints to be used for creating Web services.

Web services that conform to the REST architectural style, called RESTful Web services, provide interoperability between computer systems on the Internet.

REST is not a standard in itself, but RESTful implementations make use of standards, such as HTTP, URI, JSON, and XML.

Figure 12 shows Adaptor-Node Interface, reporting the elements described above.

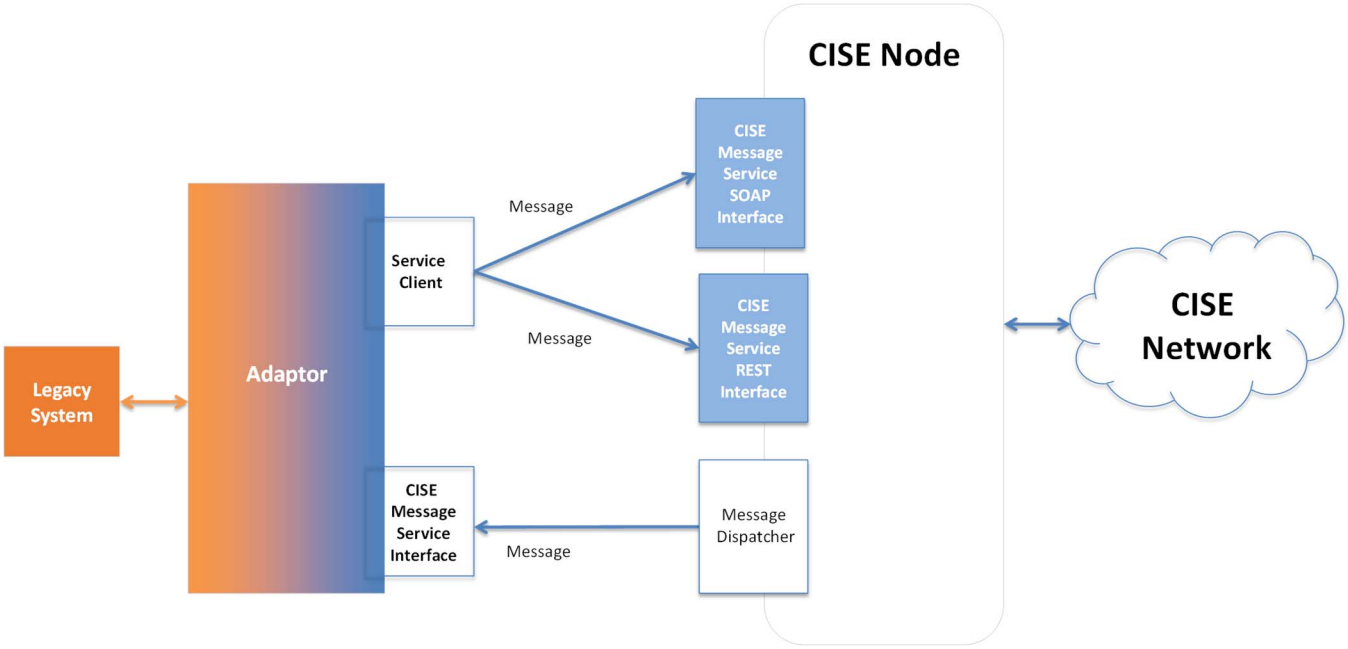

Figure 12: Adaptor-Node interface

5.2.3 The Node to Node communication

The CISE network shall be designed as a global peer-to-peer network without any central component managing the communications between nodes.

A private virtual network shall be 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.

CISE infrastructure shall implement TCP based transport layer (IETF RFC 793 [3]) and IP based network layer (IETF RFC 791 [4]) to support the communications between CISE Nodes and Adaptors.

Within the virtual network, there shall be no routing. If Node X wants to communicate with Node Y, a separate VPN-tunnel from X to Y shall be established.

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). Once configured, the routers/firewalls shall maintain a constant tunnel between them that links the different sites. In this scenario, users do not do anything to initiate the VPN session because it is always on (see Figure 13).

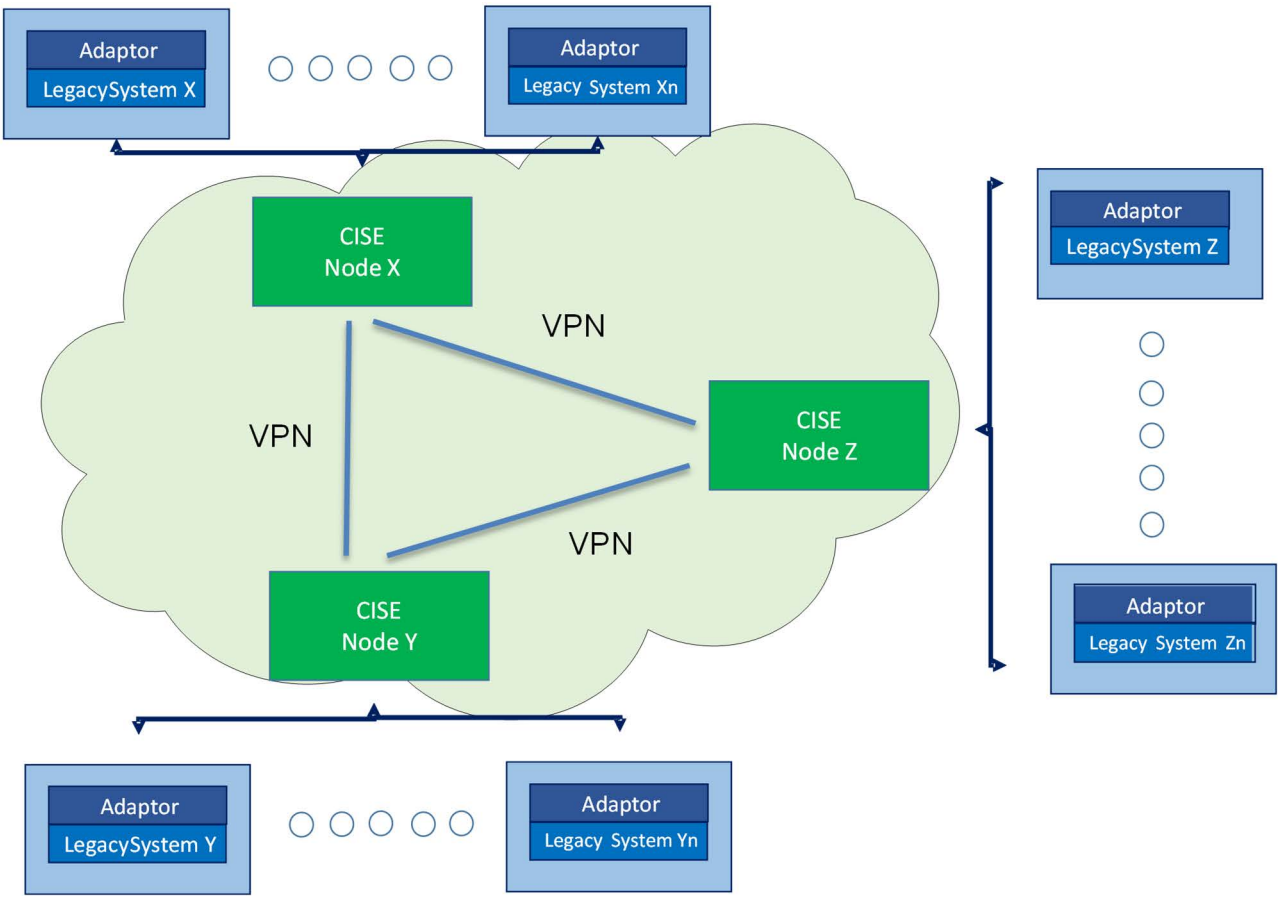

Figure 13: CISE Site-to-Site VPN connection

In the VPN topology, each Site is connected to all other Sites.

Each of the VPN tunnels between two CISE Sites shall use a state-of-the art security configuration.

NOTE: Possible configurations are listed in Annex A.

The CISE components shall be able to handle both unclassified and classified information up to EU Restricted level.

CISE Nodes dealing with CLASSIFIED information shall be installed on Sites in the CLASSIFIED physical network with the same classification level.

The following Figure 14 shows that CISE shall have two separate networks, one for UNCLASSIFIED information and one for CLASSIFIED (up to EU RESTRICTED Level) information.

The CISE shall not exchange any message between its networks (both way).

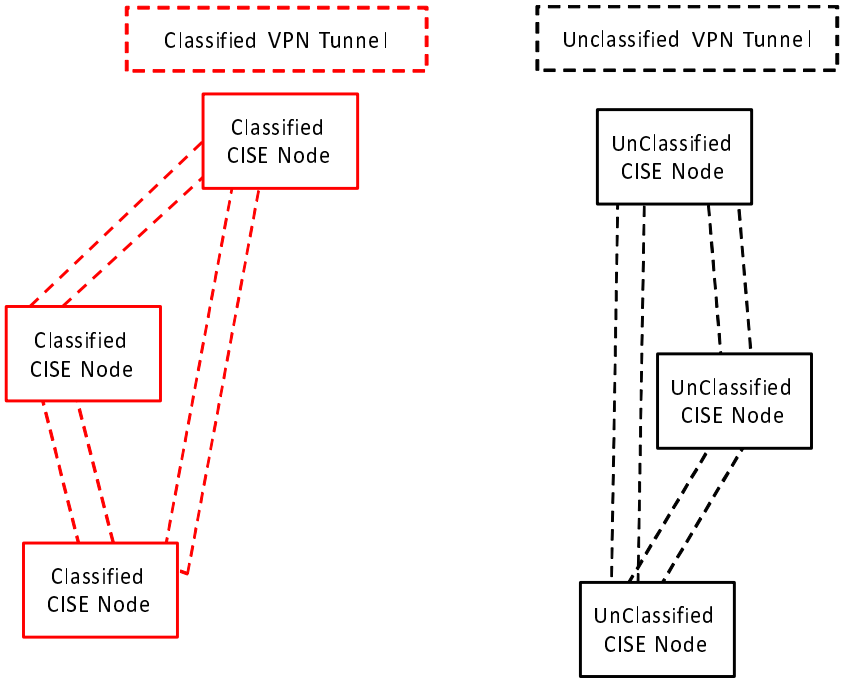

Figure 14: CISE CLASSIFIED and UNCLASSIFIED Networks

CLASSIFIED network deals with sensitive information that needs to be protected and does not have to be made available to the unclassified network. CLASSIFIED network shall use cryptographic protocols and standards in order to ensure the confidentiality and integrity of the data.

In site-to-site communications, CLASSIFIED network shall use certified crypto device and site-to-site Virtual Private Network (VPN) to secure data in transit across untrusted network.

Certified Crypto device shall be compliant with Council as Crypto Approval Authority (CAA), as reported in [i.3].

5.2.4 The Adaptor to Node communication

The communication between adaptors and nodes shall be secured. If the two components are not hosted on the same site, a VPN communication with the same level of security as the Node to Node communication shall be established.

Participants shall be requested to use VPN for Adaptor-Node communication, with TLS encryption as well:

- TLS encryption shall be enabled by using Node's CA Certificate chain (SSL).
- All adaptors connected to the Node shall connect using SSL service.
- The collaborative tool shall use TLS.

5.3 Service Description

5.3.1 General Requirements

CISE Services shall fulfil the requirements defined in clauses 5.2 and 5.3 of ETSI GS CDM 002 [1].

CISE network shall be able to offer services for data exchange between a heterogeneous set of legacy systems using a common data model.

Data shall be exchanged by the legacy systems through the interface components called Adaptor.

The task of the Adaptor shall be to ensure the acquisition of information from the legacy systems, normalizing data according to the CISE data model, and invoking the Interface Services.

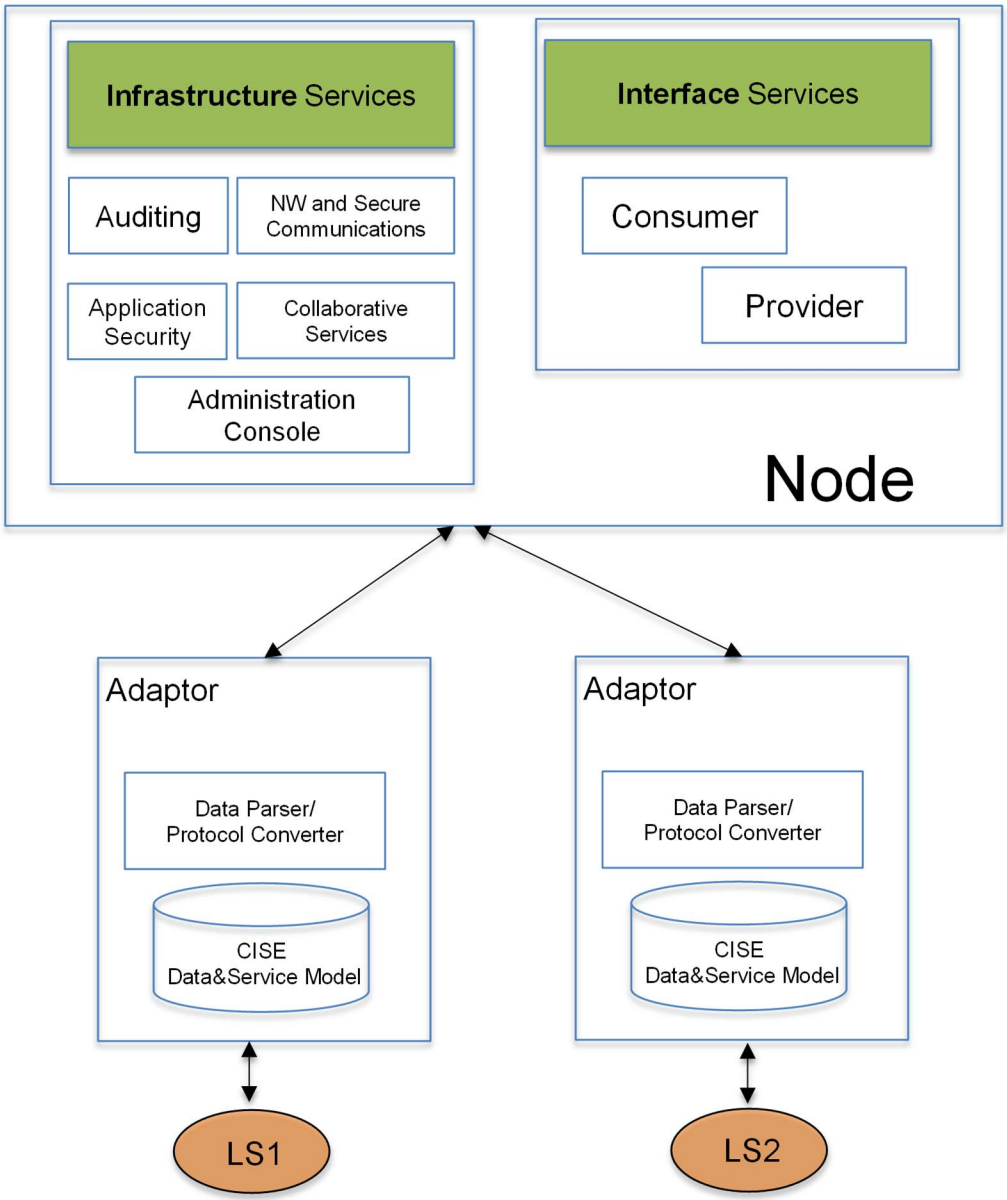

Figure 15: CISE Services Environment

Figure 15 shows the organization of CISE Services in two classes:

1) Infrastructure services: devoted to enable the connection of the CISE Participants.

2) Interface services: dedicated to the transfer of entities within the CISE network following the CISE service and data models.

Figure 16 describes all the services composing the Infrastructure and Interface Services, which shall be implemented in the Node.

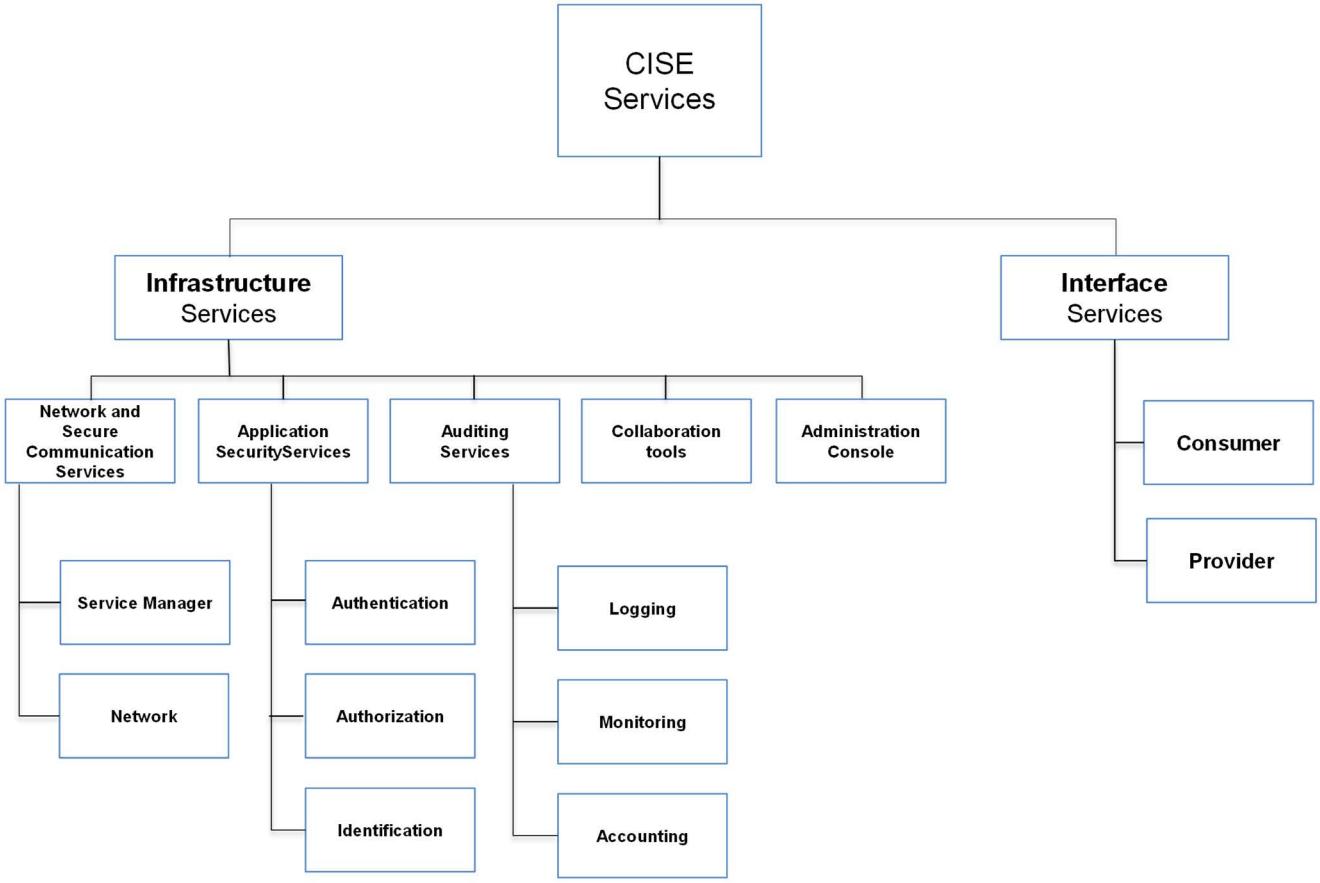

Figure 16: CISE Services

5.3.2 Infrastructure (Core Services)

5.3.2.1 Infrastructure Introduction

Infrastructure services are defined as follows:

- 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.

5.3.2.2 Auditing Services

The purpose of the Auditing Services is to perform analysis on events, tasks and actions performer.

The auditing services shall fulfil the requirements defined in clause 5.2.6 of ETSI GS CDM 002 [1].

Auditing Services shall be as described in the following Table 1, on the bases of Logging, Accounting and Monitoring.

Table 1: Auditing Services description

Auditing Services	
Service Name	**Description**
Logging	This service logs all the activity of the system.
Accounting	This service tracks all requests that come through the CISE network, recording information like consumer and provider community, data and purpose of request.
Monitoring	This service tests automatically and periodically the availability and effectiveness of the CISE services.

The logging service shall save the minimum set of logging information described in Table 2.

Table 2: Logged information

Logging Service	
Parameter name	**Description**
message_context_id	Message context Identification
message_correlation_id	Correlation Identification used in various service for message
message_id	Identification of Message
service_id	Service Identification
log_message	The high level name of the LOG code
trace_log_details	The detailed description of the LOG code
message_creation_date_time	The date of log generation
log_level_type	Log Level Types (DEBUG, INFO, WARN, ERROR, FATAL)

The Accounting Service shall save the minimum set of information described in Table 3.

Table 3: Information saved by the Accounting Service

Accounting Service	
Parameter name	**Description**
message_context_id	Message context Identification
message_correlation_id	Correlation Identification used in various service for message
message_id	Identification of Message
operation_category	The operation of the Message (Push Known, Push Unknown, Pull Request Known, Pull Request Unknown etc)
message_creation_date_time	The creation date of the message
has_personal_data	Flag indicating the payload of the message as personal data
sender	Sender service details (see table 3)
recipient	Recipient service details (see table 3)
operational_purpose	The operational purpose of the message
entities	The List of entities exchanged within message (see table 4)

The Accounting Service shall have the minimum set of message information described in Table 4.

Table 4: Message Information saved by the Accounting Service

Message Information	
Parameter name	**Description**
service_id	The id of the service
service_type	The type of the service with regards to entities which can be exchanged
service_operation	The operation type of the service (push, pull, subscribe, acknowledgement, feedback)
service_role	The Role of the service (producer / consumer)
service_status	The status of the service (online, offline etc)
participant_name	The name of the participant legacy system offering the service
participant_member_state	The member state code of the legacy system offering the service
sea_basin	The sea basin operation of the service

The Accounting Service shall have the minimum set of entity information reported in Table 5.

Table 5: Entity information to be saved by Accounting Service

Entity Information	
Parameter name	**Description**
name	The simple class name of the CISE Data Model entity being exchanged
attributes	The name of the CISE Data Model entity's fields being exchanged

5.3.2.3 Application Security Services

5.3.2.3.1 Identification and Authentication Services

The Identification and Authentication services shall fulfil the requirements [Fun-IAA-01], [Fun-IAA-02] [Fun-IAA-03], [Fun-IAA-04], [Fun-IAA-05], [Fun-IAA-06] and [Fun-IAA-07] defined in clause 5.2.4 of ETSI GS CDM 002 [1].

CISE shall define at least three kinds of users:

- CISE Participant: one of the legacy systems connected and can operate as a service provider or service consumer;
- CISE Configuration Manager: responsible for the CISE Node, for the management of the services and for the definition of their Access Right Policy;
- CISE Node Administrator: responsible to add/update/delete Participants.

The authentication mechanism used to access CISE network shall be based on X.509 certificates, according to Recommendation ITU-T X-509 [2].

Dedicated PKI Certification Authorities shall issue these certificates, for both CLASSIFIED and UNCLASSIFIED networks.

Each Member State shall have its own Root Certification Authority hosted in the Node and federated with the others at application security level. 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 Node.

The Node Administrator is responsible for the registration of Participants.

Since the UNCLASSIFIED and CLASSIFIED networks are physically separated, Participants with classification CLASSIFIED, and the services they provide, are not visible to the UNCLASSIFIED ones. The two networks have separate PKI services and separate Root Certification Authorities.

Every Member State owns its PKI. Each PKI has its own trust in Certification Authority that emits the site certificates. Any CISE Node trusts the Certification Authority of all other CISE Nodes for the domain that they represent.

Figure 17 shows the relationship between any CA CISE PKI infrastructure inside CISE network.

The trust is performed adding all the Member States (that agree to participate) as trusted root certificate for the new member state.

The secure transfer of information between participants of the CISE Network can be ensured by using the XML signature, which is encapsulated in every message exchanged via CISE Nodes [i.2].

The message signature mechanism when sending a message from Adaptor A -connected to CISE Node A1- to Adaptor B -connected to CISE Node B1- consists of the following steps:

1) Adaptor A signs the whole message using its own Certificate generated by its CISE Node Trusted Authority.

- CISE Node A1 receives the message from Adaptor A and:
  - Verifies the signature of Adaptor A.
  - Signs the whole message again using the CISE Node's Certificate which is trusted by all other connected CISE Nodes.
  - Sends the message to the recipient CISE Node B1.

- Recipient CISE Node B1 receives the message from CISE Node A1 and:
  - Verifies the signature of CISE Node A1.
  - Signs the whole message again using CISE Node B1 Certificate trusted by Adaptor B.
  - Sends the message to the recipient Adaptor B.

2) Adaptor B verifies the signature of the message and processes it.

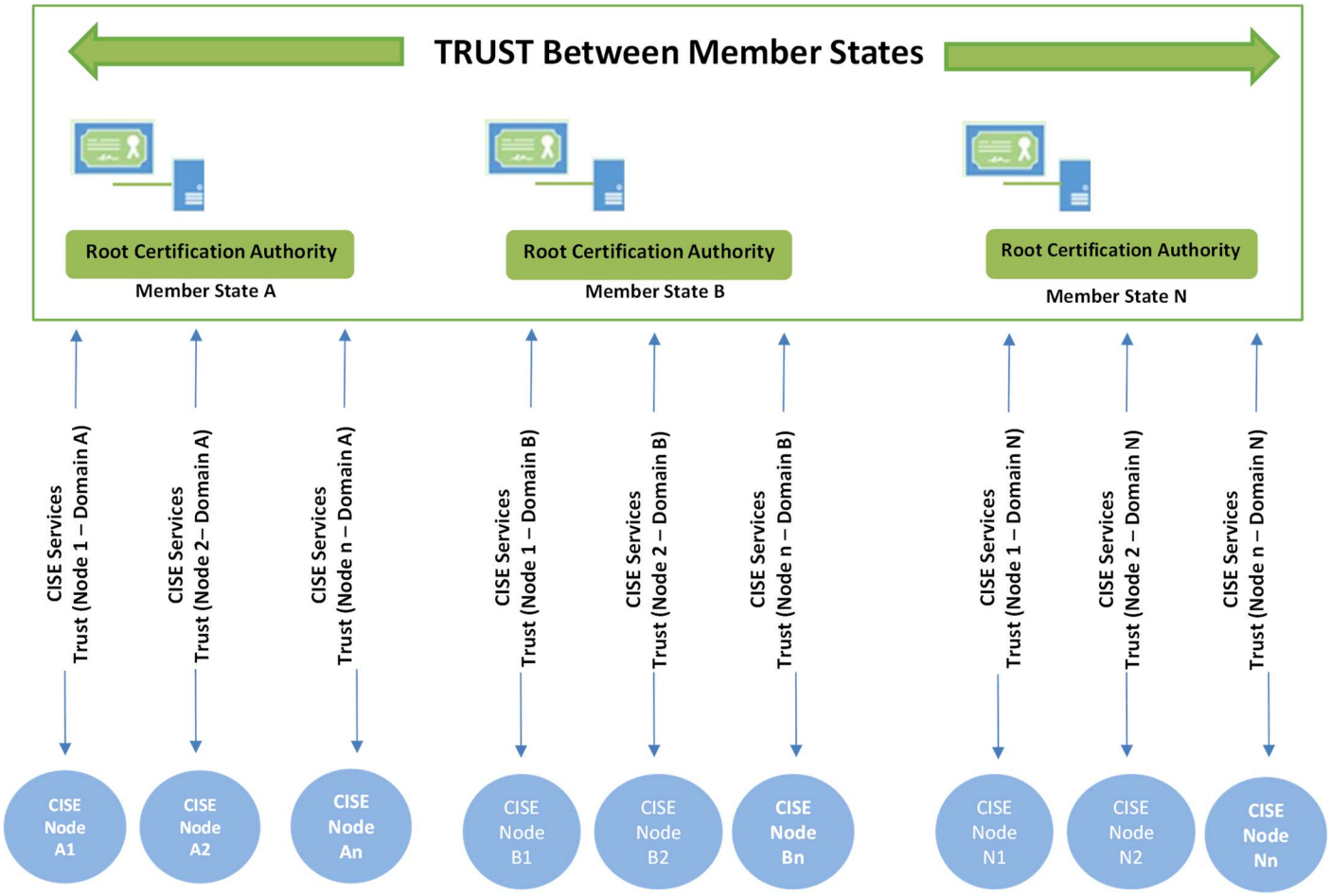

Figure 17: PKI Communication Diagram

5.3.2.3.2 Authorization Services

Authorization services shall fulfil the requirements [Fun-IAA-08], [Fun-IAA-09], [Fun-IAA-10] and [Fun-IAA-11] defined in clause 5.2.4 of ETSI GS CDM 002 [1].

Authorization shall be a distributed process performed along the network component. It shall apply to management of requests and replies to avoid useless requests.

Authorization Services shall 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, national agreements and operational purpose (Access Right Matrix).

The Configuration Manager shall populate the related Access Right Matrix in order to define the policy for the availability of the service and of each entity's attributes exchanged.

Rules shall be defined and amended by the Configuration Manager of a Node by using the Administration Console graphical user interface on the bases of:

- Participant Rules:

  In each Node the Configuration Manager shall define a set of rules for each Service published in order to define the Participants that may have access or not to it.

- Information Elements:

  In each Node the Configuration manager shall define the specific Participant List allowed to receive information elements.

- Access Right Matrix Check Flow:

  When the Participant wants to consume a service provided by another Participant (Pull request), the Provider shall check the Access Right Matrix defined by the Configuration Manager of its own Node and shall reply with a response detailing if the consumer is allowed to retrieve all or part of the available information.

If the Consumer has the right to query that service, the Provider shall return only the information elements allowed by the Access Right Matrix.

For the Subscribe the flow is similar and the authorization checks shall be performed by the Provider using the Access Right rules defined on its Node before accepting the Consumer as a valid subscriber.

When the Participant wants to provide information using the PUSH pattern of a service to another Participant, the Provider shall check the Access Right Matrix defined by the Configuration Manager of its own Node.

The message shall be delivered to the Consumer only if it is allowed in the Access Right Matrix defined above and it shall contain only the information allowed.

5.3.2.4 Network and Secure Communication Services

5.3.2.4.1 General Requirements

The Network and Secure Communication Services shall fulfil the requirements defined in clauses 5.2.2, 5.2.3 and [Fun-DM-07] of ETSI GS CDM 002 [1].

The Network service shall encrypt the network with a cryptographic protocol: IETF RFC 5246 [5] and IETF RFC 6176 [6].

5.3.2.4.2 Service Manager (or Service Discover)

The Service Manager shall fulfil the requirements defined in clause 5.2.5 of ETSI GS CDM 002 [1].

The Service Manager shall provide the capability to manage CISE Interface Services.

CISE Service Manager shall allow to:

- publish a new Service;
- update a service provided by a Participant;
- delete a service provided by a Participant;
- search for a previously published Service.

The following attributes shall define a service:

- service type (describing the entities exchanged);
- service operation (pull, push, publish/subscribe);
- service status;

- service capabilities;
- performance information (expected response time, maximum number of results, refresh rate);
- sea basin;
- service provider.

In this way a Participant, acting as a CISE Consumer, can discover services using, as filter criteria, information regarding the service itself and/or details of the Participant that provides that service, such as the Community, the Activity and the Member State to which it belongs to.

All the Nodes shall use the same interface to synchronize the service metadata of the service registry between the CISE Nodes. After each creation, update or deletion of a service, the Node shall transmit the changes to all the other Nodes of the CISE Network. The Service Manager shall manage only the services declared by its own Node. On the other hand, the Service Discovery can search on all the services declared by all the Nodes of the CISE Network.

5.3.2.5 Administration User Interface

The Administration User Interface shall fulfil the Requirement defined in clause 5.2.7 of ETSI GS CDM 002 [1].

5.3.2.6 Collaboration tools

The collaboration tools shall fulfil the requirement [Fun-CT-01] defined in clause 5.2.8 of ETSI GS CDM 002 [1].

The collaborative services shall authenticate users via the authentication service described in clause 5.2.4 of ETSI GS CDM 002 [1].

The Collaborative services are in charge to support CISE users by providing them multimedia and auxiliary tools in order to facilitate the communications and work among them.

The tools provided by the Collaboration services are the followings:

- Instant messaging: CISE users are able to send each other text messages in an easy and efficient way, in a one-to-one chat or using group chats between more CISE Participants:
  - CISE Nodes shall support and implement a XMPP server that provides Jabber-compatible clients with chatroom functionality;
  - CISE Nodes shall support and implement TLS security in their XMPP configuration;
  - CISE Nodes shall support XMPP Core functionality as defined in IETF RFC 6120 [7];
  - CISE Nodes shall support XMPP IM functionality as defined in IETF RFC 6121 [8].
- E-Mail: using a SMTP server the Collaborative services is possible to send mail to other CISE Participants and receive notifications on predefined events:
  - CISE Nodes shall implement a SMTP-compliant e-mail server for closed-loop CISE communications.
  - Each CISE Node shall have its own SMTP server.
- Video and Voice Conference: by exploiting the Collaborative services, CISE Participants can perform Video and Voice conferences between two or more CISE Participants;
  - CISE Nodes shall implement RTP - compliant (according to IETF RFC 3550 [9]) media streaming that allows for live conferencing.
  - Each CISE Node shall implement WebRTC as defined in [10].
- White Board: Collaboration services provide shared white boards in which several CISE users can draw, write, create images and clip-arts in a joint session;
- File Transfer: using FTP servers on the CISE Node is possible to send and receive files among the CISE Participants;

- Each CISE Node shall implement a FTP Server supporting both FTP and SFTP.

- Shared Documents Repository: each CISE Node has a document repository shared with the others CISE Participants by using the WebDAV protocol;
  - Each CISE Node shall implement a WebDAV- compliant documentation server as defined in IETF RFC 4918 [11].

- Shared Calendar: a CISE user can create calendar events to be shared with others CISE users and send/receive e-mail with details of the scheduled meetings:
  - Each CISE Node shall implement a CalDAV - compliant calendar server as defined in IETF RFC 4791 [12] and IETF RFC 6638 [13].

5.3.3 Interface (Common Services)

5.3.3.1 General Requirements

The exchange of information between Legacy Systems of the CISE Network is performed by Adaptors connected to a CISE Node of the Network. An Adaptor can act as Consumer or Provider of information and shall implement and expose the Common Services Interface necessary for the information verification and transfer. This Interface is also implemented by each CISE Node connected to the CISE Network to allow all connected Adaptors to send information to the CISE Node and thus the CISE Network.

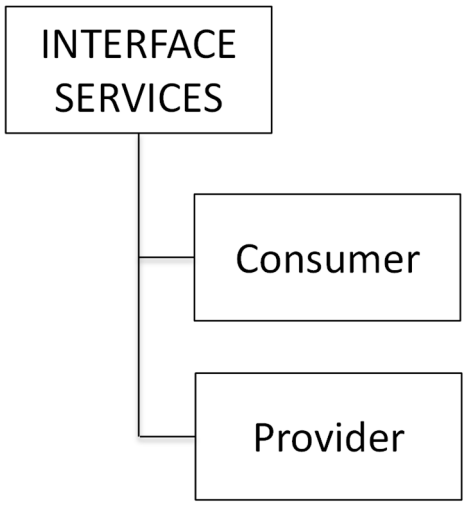

Figure 18: Interface Services

The Interface Services, shall implement the Pull, Pull Unknown Recipients, Push, Push Unknown Recipients, Publish and Subscription functions, as defined in requirements described in clause 5.2.3 of ETSI GS CDM 002 [1].

The Interface Services shall implement the access rights rules defined in requirements [Fun-IAA-08], [Fun-IAA-09] and [Fun-IAA-10], described in clause 5.2.4 of ETSI GS CDM 002 [1].

The message structure shall be implemented as defined in requirements [Fun-MS-01], [Fun-MS-02], [Fun-MS-03], [Fun-MS-04], [Fun-MS-05] described in clause 5.3.3 of ETSI GS CDM 002 [1].

5.3.3.2 Interfaces

The interfaces of a CISE Node corresponds to two categories:

1) The interfaces between the Node and the Adaptors, which allows Adaptors to send or receive messages from the CISE Network.

2) The interfaces between the Nodes, which allows the exchange of messages between CISE participants and the synchronisation of the registries between the Nodes.

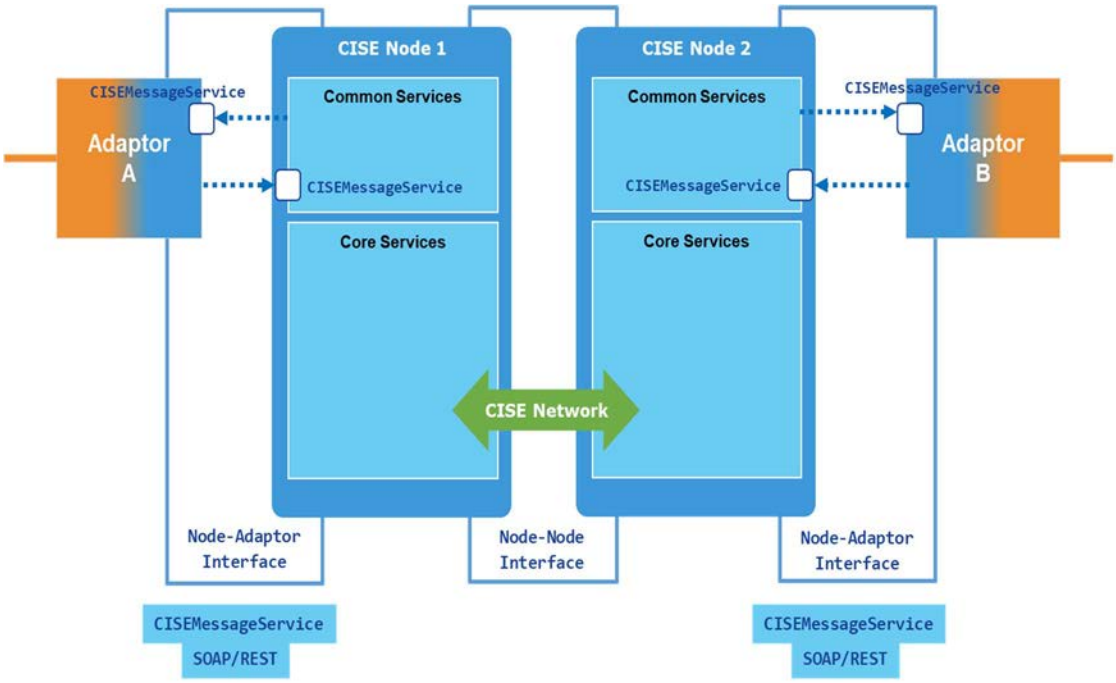

Figure 19: CISE Node Interfaces

The Adaptor-Node interface - The messaging interface

The messages exchanged between the Adaptor and the Node are of two types:

- The messages that shall be shared only between the Adaptor and the Node connected.
- The messages that shall be forwarded to other Nodes and Adaptors. In this case, the messages contain the information required to route the message and the payload (i.e. maritime surveillance information that needs to be transmitted to other participants).

The messages exchanges between an Adaptor and a CISE Node shall use the SOAP or the REST protocol. The Node shall be configurable to adapt to the SOAP or REST communication for each Adaptor directly linked to the Node.

The Node shall expose a single service (interface) to receive the message from all the Adaptors.
For each service offered, the Adaptor shall expose a single end point to receive all the messages from the Node. The Node shall be configurable to register the end point of the Adaptor's service. This information shall not be distributed to the other Nodes.

The Node-Node interface - The messaging interface

The messages exchanged between the Nodes are the messages sent by the Adaptor with the information required to route the message. The messages are exchanged point to point.

The service registry interface

Each CISE Node includes a service registry which contains the descriptions of the services offered by the Node and by all the other Nodes. The Node synchronises immediately the changes of its service registry with all the other Nodes.

The participant registry interface

Each CISE Node includes a Participant Registry which contains the identification of each Legacy Systems connected to the Node. The Node shall synchronise immediately the change of its Participant Registry with all the other Nodes.

The Name resolution interface

Each CISE Node includes a DNS server for the Name resolution of the Messaging system, the synchronisation of the Service and Participant registries and the collaborative tools.

Every DNS server shall handle its own domain.

Every DNS server shall forward the requests for name resolution to the other domains.

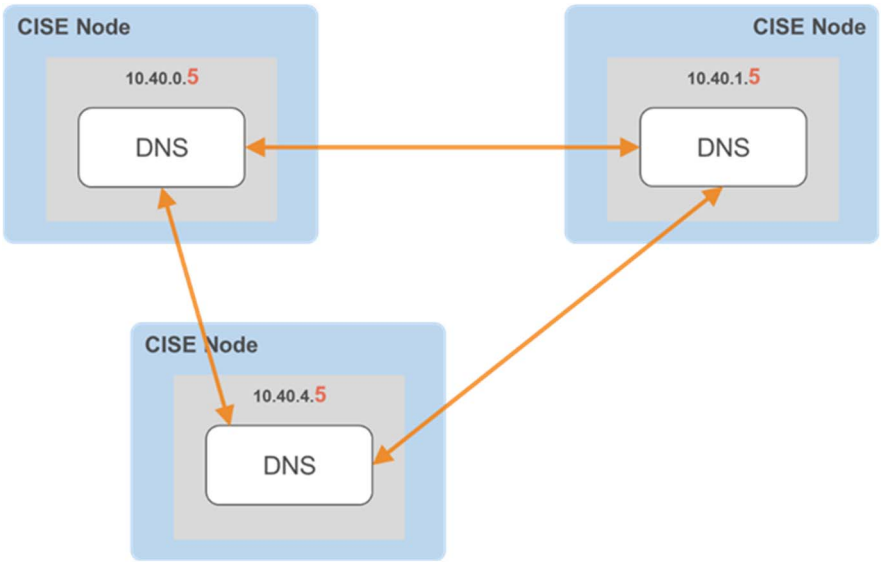

Figure 20: Name resolution between the CISE Nodes

The collaborative tools interface

The collaborative tools of the CISE Node consist of standalone open-source 3rd party tools which are offering their own Web-based User Interfaces. The collaborative tools are integrated with the CISE Node's Identification Services re-using the CISE Node Participant Registry as their user catalogue.

5.4 CISE Performances

Performance requirements shall be compliant with clause 6 of ETSI GS CDM 002 [1].

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 and Figure A.2).

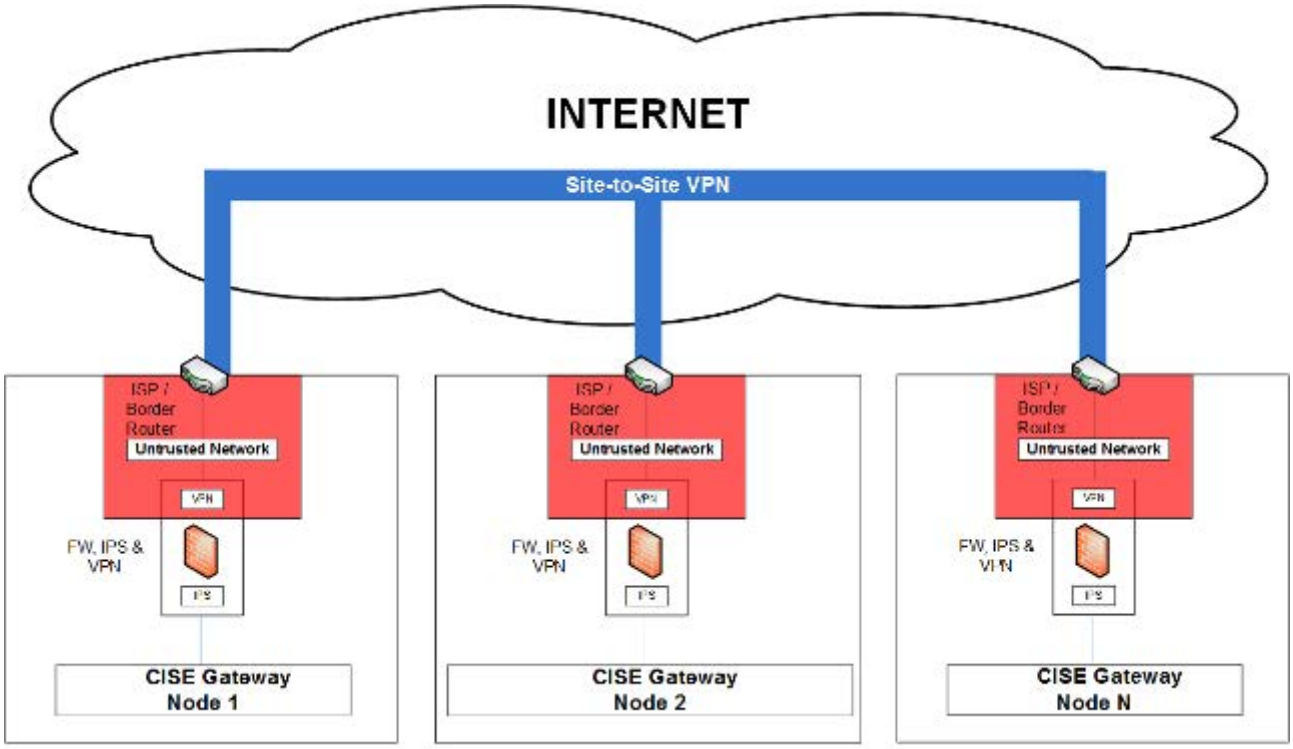

Figure A.1: CISE Site-to-Site VPN's concept (1)

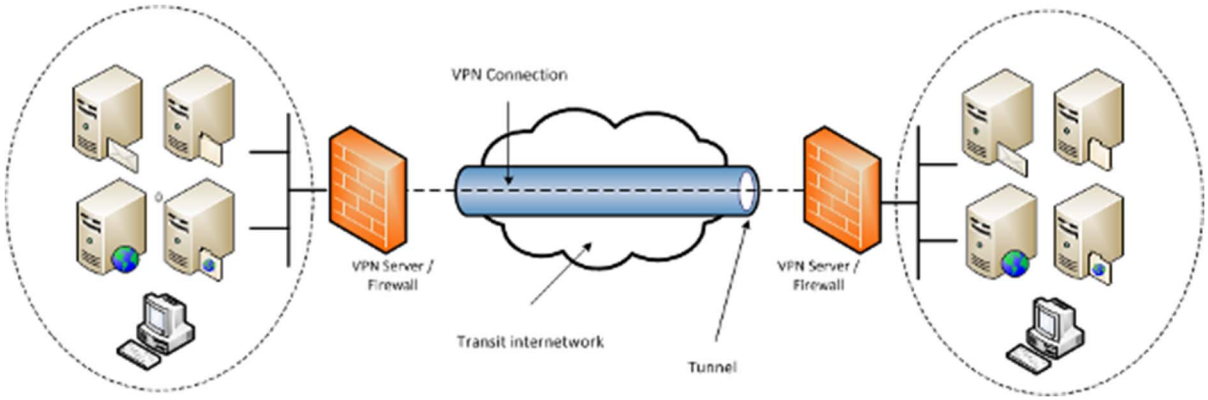

Figure A.2: CISE Site-to-Site VPN's concept (2)

A.2 Configuration A

Table A.1 shows a VPN configuration that is allowed.

Table A.1: Allowed VPN configuration for the CISE Network

Allowed IPSEC parameters for CISE Network	
Parameter Description	**Allowed**
Mode	Tunnel
IKE Version	1 (in main mode)
IKE Mode	main
Psk length	45 chars
DH Exchange	modp4096 – Group 16
AH Hashing	HMAC-SHA2-512
Phase 1 Hashing	HMAC-SHA2-512
Phase 1 Encryption	AES-128
Key Lifetime	7 200 s
Phase 2 Hashing	HMAC-SHA1
Phase 2 Encryption	AES-256-gcm
Key Lifetime	43 200 s
Perfect Forward Secrecy	enabled

A.3 Configuration B

The preferred VPN configuration is show in Table A.2.

Table A.2: Preferred VPN configurations for the CISE Network

Preferred IPSEC parameters for CISE Network	
Parameter Description	**Preferred**
Mode	Tunnel
IKE Version	2
IKE Mode	main
Psk length	64 chars
DH Exchange	ecp192 - Group 25
AH Hashing	HMAC-SHA2-512
Phase 1 Hashing	HMAC-SHA2-512
Phase 1 Encryption	AES-256
Key Lifetime	3 600 s
Phase 2 Hashing	HMAC-SHA2-512
Phase 2 Encryption	AES-512-gcm
Key Lifetime	7 200 s
Perfect Forward Secrecy	enabled

History

Document history		
V1.1.1	May 2021	Publication