



TECHNOLOGICAL HANDBOOK

Framework for Smart Maritime Information
Exchange

ABSTRACT

This document aims to support the decision making processes and the technological activities necessary to exchange information through the national maritime information exchange environment (NIPIM@R). Hence, it comprises the technical information necessary for achieving that purpose.

Directorate-General for Maritime Policy
PORTUGAL

December 07, 2015

Revision history

Rev.	Date	Author	Notes
0.1	October 27, 2015	MARQUES, Fernando	Structure and introduction.
0.2	October 28, 2015	MOTA, Bernardino	Architecture and integration strategy.
0.3	October 29, 2015	MARQUES, Fernando	Integration strategy principles
0.4	October 30, 2015	MARQUES, Fernando	Overall review.
0.5	November 8, 2015	MOTA, Bernardino	Additional contents for Architecture and integration strategy.
0.9	November 26, 2015	MOTA, Bernardino	Overall enhancement
1.0	December 4, 2016	PINTO, Hugo; MARQUES, Fernando	Overall review and release approval

Contents

Revision history	2
Contents	3
List of tables.....	5
List of figures	6
Glossary	7
1 Introduction	10
1.1 NIPIM@R.....	12
1.2 Smart interoperability	13
1.3 Overview	15
2 Architecture.....	16
2.1 Principles	16
2.1.1 Business principles	16
2.1.2 Applications, services and data principles.....	17
2.1.3 Technology principles.....	18
2.2 Vision.....	19
2.3 Overview	19
2.3.1 Business View	24
2.3.2 Application View.....	36
3 Integration strategy.....	46
3.1 NIPIM@R Gateway.....	46
3.2 NIPIM@R Data Model	52
3.3 NIPIM@R Web Services Model	58
3.3.1 Message Exchange Patterns	61
3.3.2 Message Identifiers	63

3.3.3	Query base mechanism	63
3.4	Security model.....	66
3.4.1	NIPIM@R Gateway to/from NIPIM@R National Node.....	66
3.4.2	NIPIM@R Gateway to/from Operational Systems	66
4	References.....	68
	Appendix 1 – Data model specifications (XSD).....	69
	Appendix 2 – Information services specifications (WSDL)	70
	Appendix 3 – Archimate Quick Reference Guide	71

List of tables

Table 1 – Business Roles.....	25
Table 2 – High level generic process to Exchange information.....	28
Table 3 – Sub process “Submit Message”	29
Table 4 – Application Service used by Sub process “Submit Message”	30
Table 5 –Sub process “Send Message”	31
Table 6 – Application Service used by sub process “Send Message”	31
Table 7 –Sub process “Manage Message Transport”	33
Table 8 – Application Service used by sub process “Manage Message Transport”	33
Table 9 –Sub process “Receive Message”	34
Table 10 – Application Service used by sub process “Receive Message”	35
Table 11 –Sub process “Accept Message”	36
Table 12 – Application Service used by sub process “Accept Message”	36
Table 13 – Core Application Services	40
Table 14 – Common Application Services	42
Table 15 – Custom Application Services.....	44
Table 16 – Organization Application Services	45
Table 17 – Integration protocols	51
Table 18 – Services vs Patterns	60
Table 19 – Services operations.....	60

List of figures

Figure 1 – A high level example for information exchange without NIPIM@R.....	20
Figure 2 - A high level and simple example for information exchange with NIPIM@R..	21
Figure 3 – High level picture of NIPIM@R.....	22
Figure 4 – Placement of Business Actors.....	25
Figure 5 - High level process for information exchange.....	26
Figure 6 – Sub process “Submit Message”.....	29
Figure 7 – Sub process “Send Message”.....	30
Figure 8 – Sub process “Manage Message Transport”.....	32
Figure 9 – Sub process “Receive Message”.....	34
Figure 10 – Sub process “Accept Message”.....	35
Figure 11 – Categories of Application Services.....	37
Figure 12 – NIPIM@R building blocks and application services.....	38
Figure 13 – Example screenshots of the GUI for Maritime Info.....	42
Figure 14 – Example 1 for deployment of NIPIM@R Gateway.....	47
Figure 15 – Example 2 for deployment of NIPIM@R Gateway.....	48
Figure 16 – Data model core entities.....	54
Figure 17 – Pull pattern.....	62
Figure 18 – Push pattern.....	62
Figure 19 – Publish/Subscribe pattern.....	63
Figure 20 – Query-by-example.....	64
Figure 21 – Structured query.....	65
Figure 22 – Overview of the security boundaries.....	66

Glossary

This glossary briefly explains the terms that can be found along the document.

A

<i>AIS</i>	<p>Automatic Identification System (AIS)</p> <p>Is an automatic tracking system used on ships and by vessel traffic services (VTS) for identifying and locating vessels by electronically exchanging data with other nearby ships, AIS base stations, and satellite</p> <p>Source: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx</p>
<i>API</i>	<p>Application Programming Interface (API)</p> <p>Is a set of routines, protocols, and tools for building software applications.</p>
<i>ArchiMate®</i>	<p>ArchiMate®, an Open Group Standard, is an open and independent modelling language for enterprise architecture that is supported by different tool vendors and consulting firms. ArchiMate provides instruments to enable enterprise architects to describe, analyse and visualize the relationships among business domains in an unambiguous way.</p> <p>Source: http://www.opengroup.org/</p>
<i>ASTERIX</i>	<p>All Purpose STructured Eurocontrol SuRveillance Information Exchange</p> <p>It is an ATM Surveillance Data Binary Messaging Format which allows transmission of harmonised information between any surveillance and automation system.</p> <p>Source: http://www.eurocontrol.int/asterix</p>

B

<i>BB</i>	<p>Building Block</p> <p>A building block represents a (potentially re-usable) component of business, IT, or architectural capability that can be combined with other building blocks to deliver architectures and solutions.</p> <p>Source: http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html</p>
<i>BP</i>	<p>Business Process</p> <p>A structured, measured set of activities designed to produce a specific output for a particular customer or market. It implies a strong emphasis on how work is done within an organization, in contrast to a product focus's emphasis on what. A process is thus a specific ordering of work activities across time and space, with a beginning and an end, and clearly defined inputs and outputs: a structure for action.</p>

Source: Thomas Davenport (1993). Process Innovation: Reengineering work through information technology. Harvard Business School Press, Boston

C

<i>CISE</i>	Common Information Sharing Environment European interoperability layer for cross-sectorial and cross-border maritime information sharing. Source: http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance
-------------	--

D

<i>DMZ</i>	Demilitarized Zone Is a physical or logical sub network that contains and exposes an organization's external-facing services to a larger and untrusted network.
------------	--

E

<i>EAI</i>	Enterprise Application Integration
<i>EC</i>	European Commission

G

<i>GTW</i>	Gateway A product or feature that uses proprietary techniques to link heterogeneous systems. Source: http://www.gartner.com/it-glossary/gateway/
------------	--

N

<i>NGTW</i>	NIPIM@R Gateway
<i>NN</i>	National Node
<i>NNN</i>	NIPIM@R National Node

O

OS

Operational System

System that is used to process the day-to-day transactions of an organization.

U

UML

Unified Modeling Language™

The OMG's Unified Modeling Language™ (UML®) helps you specify, visualize, and document models of software systems, including their structure and design, in a way that meets all of these requirements.

Source: <http://www.omg.org/>

1 Introduction

In the scope of the Integrated Maritime Policy (IMP)¹, several studies have been carried out by the European Commission (EC) which highlight the fact that much of the information necessary for policy and decision making and for conducting activities in the maritime domain is usually not available at many of the relevant maritime authorities' information systems and, often, not available at all, although it is held by some of them.

Inevitably, such information gaps will lead to less efficient and effective results, either because relevant information is lacking or because the necessary resources to acquire, store, process and manage such information, which is already held by other authorities, are newly developed, hence incurring in duplicated and unnecessary costs.

Consequently, the EC has launched the maritime Common Information Sharing Environment (CISE)² initiative with the purpose of enabling cross-sectorial and cross-border information sharing.

The CISE is therefore an interoperability instrument and, as such, comprises the organizational, legal, technical and semantic layers, which are being developed by the EC in the context of subsidiary initiatives.

BlueMassMed was one of these initiatives, which comprised around 60 public authorities from 6 member states (Portugal, Spain, Italy, France, Greece and Malta), and contributed to the CISE by developing a legal study, a set of use cases and a technological solution consisting of 4 national nodes deployed in Portugal, Italy, Spain and France. These nodes were, in turn, connected to information systems of public authorities involved in the project and the capability of sharing maritime information, through the nodes, has been demonstrated.

¹ http://ec.europa.eu/maritimeaffairs/policy/index_en.htm

² http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm

More or less in parallel, another project was carried out, the MARSUNO³, involving northern European countries, which contributed to the CISE with several recommendations.

Afterwards, the CoopP project took place. Involving several public authorities and 12 states, it leveraged the results of the previous initiatives and contributed to the CISE with enhanced use cases, legal studies and with an information and a services model.

Based on the technological results of the CoopP and considering that these were not experimented, and also that a larger initiative (EUCISE2020) was being prepared, an initiative called CISE incubator⁴ took place, involving Portugal, Italy, Norway, Germany, and several EC services, such as the JRC, DIGIT and MARE, in order to experiment with the results of the CoopP, namely the data model and services. Several conclusions have been drawn and recommendations were presented.

Presently, the EUCISE2020⁵ is ongoing, involves over 60 public authorities from 15 European states, and aims to deliver a European initial operational capability for cross-sectorial and cross-border maritime information sharing and ascertain its operational benefits. This technological layer is expected to be deployed in at least 10 of the participating states and integrated with information systems from the participating authorities.

In 2014, the European Union Maritime Security Strategy (EUMSS)⁶ has been developed and maritime information sharing, more specifically the CISE, has been considered one

³ http://ec.europa.eu/newsroom/mare/itemdetail.cfm?subweb=342&lang=en&item_id=8669

⁴ https://joinup.ec.europa.eu/software/digit_cise/wiki/digit-common-information-sharing-environment-cise-incubator

⁵ <http://www.eucise2020.eu/>

⁶ http://ec.europa.eu/maritimeaffairs/policy/maritime-security/index_en.htm

of its essential pillars, which led to several related actions being included in the action plan⁷ that followed.

Last but not least, the potential of the CISE towards the interoperability of the European public administrations dealing with information from the maritime domain was recognized by the Digital Agenda for Europe⁸ and, presently, the two flag initiatives EUCISE2020 (MARE) and eSENS (CONNECT)⁹ are working together aiming mutual benefits.

1.1 NIPIM@R

Portugal has been participating in the CISE related initiatives since the first moment, involving over 12 public authorities coordinated by the Directorate-General for the Maritime Policy (DGPM).

In this context, Portugal has been developing a national maritime information exchange environment (NIPIM@R), aiming, in first place, the cross-sectorial exchange of maritime information, at the national level, and in second place, the cross-border exchange of maritime information, through the CISE, hence contributing significantly to it.

The NIPIM@R is an initiative comprised by the National Ocean Strategy¹⁰ action plan which contributes to the national developments related to the IMP and to the national digital agenda as well.

This project involves over 12 public authorities and aims the development of the organizational, legal, technical and semantic interoperability layers among them. In this context, several initiatives have been carried out, being the most prominent one the development of the technological infrastructure to support the sharing of maritime information across the systems of the public authorities involved.

⁷ http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

⁸ <http://ec.europa.eu/digital-agenda/en/>

⁹ <http://www.esens.eu/home/>

¹⁰ http://www.dgpm.mam.gov.pt/Pages/ENM_2013_2020_EN.aspx

This technological infrastructure is up and running since 2012, when it was the national node of the BlueMassMed project. Presently, it integrates the AIS system of the Navy and the VMS system of the DGRM. Moreover, it has been used in several experimentations such as the REP military exercises or the CISE Incubator, where additional capabilities have been experimented, the most notable of which being the streaming of video provided by Air Force UAV's.

The national node also supports the development of many initiatives related to maritime surveillance and monitoring, such as projects being developed within the EEA Grants PT02 program for Integrated Marine and Coastal Waters Management¹¹ which aims to support the Marine Strategy Framework Directive (MSFD)¹².

In 2016, three projects will start which will highly contribute to NIPIM@R. The first one, project 501 (YIN), aims the development of a national action plan for enhancing maritime information exchange via the NIPIM@R. The second one, project 602 (SINKER), aims the development of innovative services for maritime information exchange among 7 national authorities. The last one, project 703 (YAARP), aims the development and certification, according to ISO27001:2013, of an Information Security Management System for maritime surveillance information exchange.

1.2 Smart interoperability

Interoperability can be implemented in many different ways, some of which are better than other. When interoperability is implemented in the most efficient way, we call it smart, and this is one of the purposes of NIPIM@R.

Presently, we can find many examples of maritime information exchanges, among public authorities, which are based on the bilateral and dedicated integration of the relevant information systems. Whenever this happens, a new project is launched, and a new set

¹¹ http://www.dgpm.mam.gov.pt/Pages/eea_grants_projects.aspx

¹² <http://www.msfd.eu/>

of components, usually comprising hardware, software and communications services, is developed implying additional investment and operational costs.

Some of these costs are related to the “translation” which is necessary to implement between the existing information models, assuming that the organizations involved do not use a common information model for maritime surveillance information, which is often the case. Therefore, whenever a bilateral initiative exists, new components for dealing with the specific “translation” requirements have to be developed, and maintained, by those involved.

Firstly, the NIPIM@R uses a common information model (CIM), developed in the context of the European initiatives aforementioned, for conveying information from one authority to the other. This means that once a “translation” between one information model of one authority and the CIM is established, no other “transformations” have to be implemented for this particular information model, which reduces exponentially the investment and operational costs of the components supporting those “translations”.

Secondly, once the connectivity is established between an information system from one public authority and the NIPIM@R, no other initiatives are necessary to connect with other authorities, since all of them will be connected through the NIPIM@R. As such, this also decreases exponentially the investment and operational costs inherent to the integration of different information systems from different authorities.

Thirdly, there are capabilities (i.e. data fusion, correlation) that might interest several authorities and, if developed individually, will incur into multiple costs. In these cases, the NIPIM@R can be used as an infrastructure for the development and deployment of capabilities which can be shared among several authorities, thus reducing, again, significantly the investment and operational costs of those capabilities.

Finally, the NIPIM@R presents also advantages when it comes to the costs inherent to bandwidth. For example, let’s suppose an authority wishes to make available a video streaming service for other authorities to follow up a specific action. In this case, the authority providing the service will have to make available the necessary bandwidth to

ensure the quality of a service which users can vary and intermittent. If such service is made available through the NIPIM@R, the authority providing the service will not have to worry with this, since the NIPIM@R will relay the video streaming to the interested authorities, hence ensuring the necessary bandwidth itself. The big difference is that the bandwidth available at the NIPIM@R can be pooled and shared in a much more efficient way than it would be if each authority was doing it by itself.

For all the above, the NIPIM@R is a good example of smart interoperability, and can contribute significantly to the reduction of costs public authorities willing to share maritime information presently have and might incur into, if they opt for bilateral initiatives.

1.3 Overview

The rest of this handbook is organized as follows. In chapter 2 –Architecture, the overall architecture of NIPIM@R is presented; and in chapter 3 – Integration strategy, lie the detailed possibilities that can be adopted by any organization for exchanging information through NIPIM@R.

Last, but not least, this handbook is a living document, developed to and, especially, by those participating or willing to join this national maritime information sharing community; hence, all contributions to improve it are more than welcome.

2 Architecture

Before diving into the specifics of information exchange through NIPIM@R, it is important to understand the high level architecture. Therefore, this chapter describes its architecture through a set of functional and technical views depicting the structures, components, behaviours and links between its various parts, as well as its relationships with its actors.

For this purpose, several diagrams have been developed using mostly the ArchiMate® notation, the Unified Modelling Language™ (UML) and other auxiliary representations. For additional information regarding this notation consult the quick reference guide in Appendix 3 – Archimate Quick Reference Guide.

2.1 Principles

The following principles are general rules and guidelines, intended to be enduring and seldom amended, that govern the NIPIM@R's architectural process, affecting its development and maintenance.

2.1.1 Business principles

1. Interoperability - The main purpose of the NIPIM@R is to foster and support the interoperability of all organizations involved, in order to enable the maritime information exchange among them. It is not a new operational system; rather, it supports and enhances the existing ones with more and better information.
2. Inclusiveness – All national organizations interested in exchanging maritime information through the NIPIM@R are able to do so.
3. Collaborative – The NIPIM@R is a technological infrastructure to foster the collaboration among the organizations willing to exchange information through it; hence, it is also governed in a collaborative way by them.
4. Voluntarism – Exchanging information through the NIPIM@R is a voluntary act.

5. Reliability – The cornerstone of exchanging information through the NIPIM@R is trust. All organizations must rely that the information exchange agreements are fully respected.
6. Confidentiality - NIPIM@R must ensure the confidentiality of the information during transmission and put in place security measures to prevent unintended users or malicious entities to consume, produce or have access to information being transferred.
7. Simplicity – Exchanging information through the NIPIM@R must be as simple as possible, provided that the objectives are achieved. Unnecessary complexity has always negative impacts and can work as a demotivation factor; hence, it is undesired.
8. Sustainability – The sustainability of all options must be considered and ensured beforehand.
9. Availability – Those exchanging information through the NIPIM@R must be assured that it is available as agreed upon.
10. Integrity – NIPIM@R must ensure that the information has not been improperly tampered with, when registered in a database, or when in transit between system components.

2.1.2 Applications, services and data principles

1. Common Information Model – The NIPIM@R must support the exchange of information based on a common information model, in line with the CISE initiative.
2. Common Services – The NIPIM@R must support the exchange of information based on a common services model, in line with the CISE initiative. Any other services supported by the NIPIM@R can be considered, essentially for enabling the integration of existing systems in the most cost-effective way, or where the common services do not apply, provided that open standards and architectures are used.
3. Centralized commonalities – The NIPIM@R must implement an architecture based on a logical central node (the National Node), through which all

information exchanges will occur. The common capabilities should be offered by the node, hence decreasing the information exchange costs.

4. Decentralized specificities – The NIPIM@R must implement an architecture in which the specificities of the systems integrating with it are dealt with away from the node, in order to decouple them from each other. This should be achieved using Gateways, deployed at each of the organizations exchanging information through the NIPIM@R. This will decrease the information exchange costs and facilitate the integration when it comes to information security.
5. Data retention – The NIPIM@R is not the database of the maritime information databases. Therefore, it shall not retain any data exchanged among the organizations, unless technical aspects (i.e. performance and security), which have been specified and approved by the organizations involved beforehand, require it.
6. Resiliency – The NIPIM@R must adopt the necessary technological solutions to ensure the quality of service agreed upon.
7. Flexibility – The NIPIM@R should be flexible enough to seamlessly adapt to the reality and changes on the organizations exchanging information through it, and refrain, as much as possible, from impacting those.

2.1.3 Technology principles

1. Openness – The NIPIM@R is based on open technologies, standards and architectures.
2. Asynchronous – Asynchronous communication protocols should be preferred, unless they do not satisfy operational requirements (i.e. video streaming).
3. Convergence – All the NIPIM@R specifications must be inline, as much as possible, with those used by the CISE initiative and with the Digital Agenda.

2.2 Vision

NIPIM@R is presently a fault tolerant and high performance infrastructure, developed by the DGPM, with the collaboration of several organizations, for their use, and according to their requirements, in line with the CISE and the Digital Agenda.

To support and increase maritime information exchange, among civilian and military, governmental and non-governmental organizations, in the most cost-effective way, the NIPIM@R will increase their technical and semantic interoperability, by making use of proven open standards and technologies.

The national node has been, and will continue to be, an instrument of the national IMP and a support for the national maritime security, as well as of its European related initiatives. It has been and will continue to be an open initiative, involving and governed together by the national organizations willing to do it.

Up until 2020, we expect to have all national organizations that presently deal with maritime information exchanging it, as adequate, through the NIPIM@R. Simultaneously, we expect to have the NIPIM@R connected to other relevant initiatives, such as the CISE, hence enabling information exchange among all the organizations involved, as necessary. Ultimately, the NIPIM@R will contribute to a better maritime governance in Portugal and in other friend states.

2.3 Overview

The Architecture Overview presented in this chapter is represented by a set of different but complementary views that together aim to facilitate the knowledge acquisition about NIPIM@R, its main components and functions relevant to the process of information exchange.

Despite not being the purpose of this document to describe in detail all the architectural and technical aspects of NIPIM@R, like for example deployment aspects, internal hardware and software configurations, it is nevertheless important to present some of

the views that are relevant to understand the interoperability features and capacities of NIPIM@R and their relation with the involved actors.

Before entering in detail in the architectural views it is important to describe the abstract representation of the high level architecture and the placement of NIPIM@R in the context of information sharing.

As represented by the following picture, in a traditional peer to peer communication the exchange of information is done directly between the organization sending data (Organization A) and the organization receiving it (Organizations B and C). For each transaction, among other things, the organizations involved must ensure the security through physical or logical measures, and the semantic compatibility of the data.

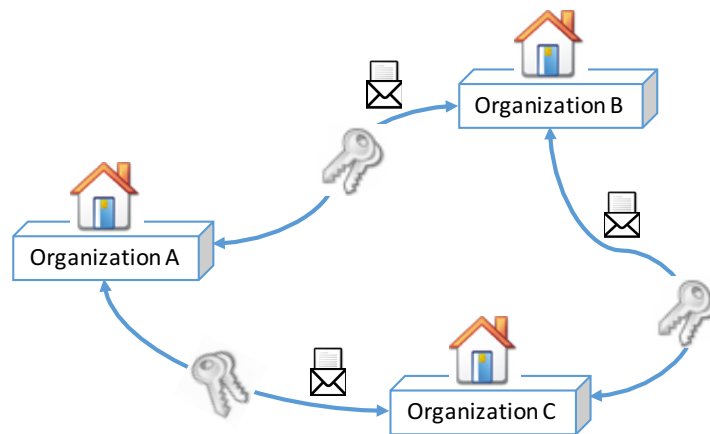


Figure 1 – A high level example for information exchange without NIPIM@R

However, as envisioned by the principles of NIPIM@R and aiming to develop “Smart Interoperability”, organizations exchanging information will use and interact with an infrastructure composed by software and hardware components that constitute the overall solution of NIPIM@R. Organizations that send and receive information are both connected to NIPIM@R, which, among other things, is responsible for accepting the information and delivering it to the final destination through secure channels and using semantically compatible data structures.

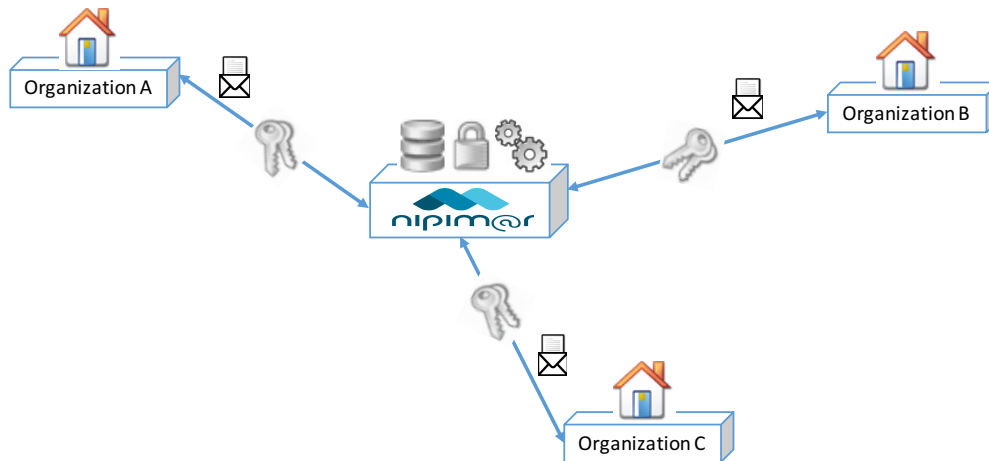


Figure 2 - A high level and simple example for information exchange with NIPIM@R

When looking more in depth to NIPIM@R, it comprises two main building blocks:

- The NIPIM@R National Node - Acts as the central element that connects with all gateways and through which all information flows.
- The NIPIM@R Gateway - The single point of access for an organization wanting to send and/or receive information. In practice, it is the only piece that connects with the organization operational systems.

As a side note, the designation “operational systems” means the organization information systems that receive or send information. They represent the information’s sources or destinations, inside the organization, which are used by its operational processes in the context of its mission and tasks.

The following picture gives a high level representation of the presented elements and their connections.

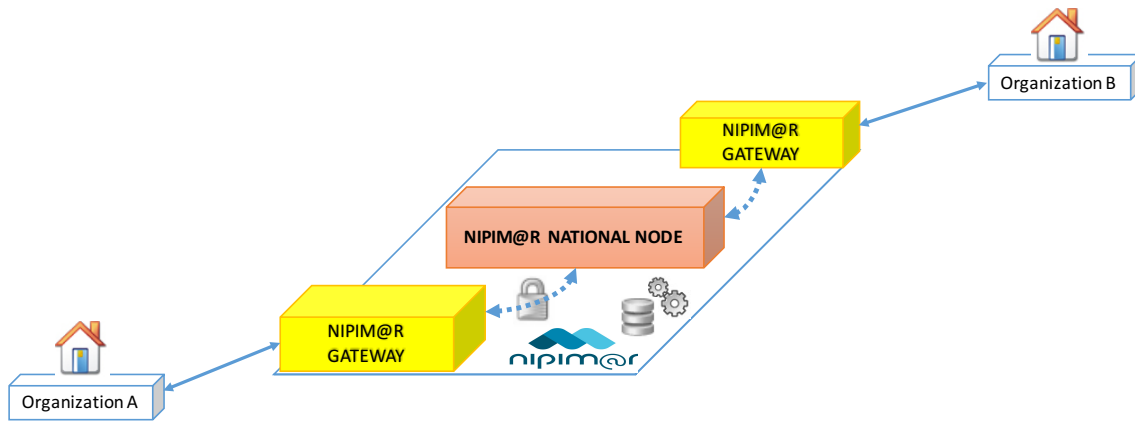


Figure 3 – High level picture of NIPIM@R

The NIPIM@R National Node is a central software component, entailing a set of auxiliary services that actively participate in the information transfer process between entities, with responsibility in the routing of information, authentication, authorization and access control management. It also holds the necessary registry repositories that supply information on the services available and the integration capabilities of each organization using NIPIM@R.

The main purpose of the NIPIM@R National Node is to centrally supply a set of capabilities and services that can be reused by organizations using the latest standards and open technologies, thus aiming to reduce the effort related with information sharing.

The National Node is redundant and supported across multiple datacentres' thus providing capacity, redundancy and fault tolerance that elevates the quality of the services offered.

The National Node is connected with NIPIM@R Gateways in a unidirectional or bidirectional manner, depending on the type of services that are used and the participation of the respective organization where they are deployed.

In this architecture, operational systems (belonging to partner organizations) transfer information through a NIPIM@R Gateway deployed at their organizations, which

function as single access point. These Gateways, in turn, never communicate with each other, but always through a central node, the National Node.

It is important to reinforce that the integration strategy between the organization (through their systems) and NIPIM@R (through the Gateway) is always decided and implemented in close collaboration with the organization representatives, and ultimately it is their decision.

If one could exemplify a very simple high level example of message transfer, it would be like this:

- 1) Organization A, sends a message to NIPIM@R Gateway A;
- 2) NIPIM@R Gateway A, forwards the message to NIPIM@R National Node;
- 3) NIPIM@R National Node, forwards the message to NIPIM@R Gateway B;
- 4) NIPIM@R Gateway B, delivers the message to Organization B

This topology, brings significant advantages regarding network segmentation. Logical and physical separation also gives partner organizations greater control over entry and exit points to their internal networks. These may be switched on and off without impact to other internal systems.

This strategy ensures the quality of a cutting-edge information exchange solution, while decreasing its costs and facilitating its adoption by the interested partners.

Over a message transfer process, several application services implemented inside the two presented building blocks are used. These application components provide core internal services and every one at its level has a specific role and responsibility in achieving the integration processes.

The following sections help to further describe the overall solution by presenting different architectural views of NIPIM@R, which are:

- NIPIM@R Business View - Business View address's the concerns of the architecture from the actor's perspective (people, organisations or systems)

when relating with operational processes involved in the exchange of information, their functions and information.

- NIPIM@R Application View - The Application View shows from a different perspective how the elements introduced and described in the Business View are in practice materialised in NIPIM@R application components.

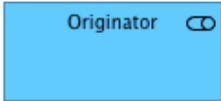
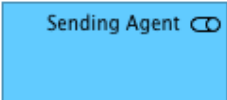
2.3.1 Business View

This Business View presents and describes the generic high level process for information exchange, the actors involved and the main services used.

When reading the figures and diagrams presented below, it is helpful to visualize them as a layered approach with the actors interacting with processes, triggering or not actions that are supported by application services. The application services will, later in the Application View, be mapped to application components.

2.3.1.1 Business roles

A business role defines a specific behaviour of a business actor participating in a given context. From the architectural point of view, NIPIM@R defines a set of Business Roles representing the main behaviours of participation in an information exchange process. The following table describes each of them.

Roles	Description
<p>Originator</p> 	<p>Has the function of triggering the submission of information to be exchanged. Usually it represents a partner organization connected to NIPIM@R.</p>
<p>Sending Agent</p> 	<p>Has the function of prepare and begin the process of information transfer to the final destination.</p>


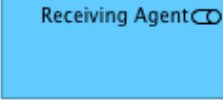
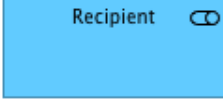
<p>Interconnect Agent</p> 	<p>This role has the responsibility to intermediate the connection between agents and do the necessary routing to deliver the information. It might do additional filtering or other actions on the information being transferred.</p>
<p>Receiving Agent</p> 	<p>Has the function of receiving the information, do additional processing regarding validation of authenticity and other security measures and, finally, delivery to the end recipient.</p>
<p>Recipient</p> 	<p>Represents the final destination for the information that was transferred and has the function to act upon the receiving data and give it the internal functional meaning.</p> <p>Usually represents the destination Organization.</p>

Table 1 – Business Roles

The following picture further enhances and positions each role in the high level picture.

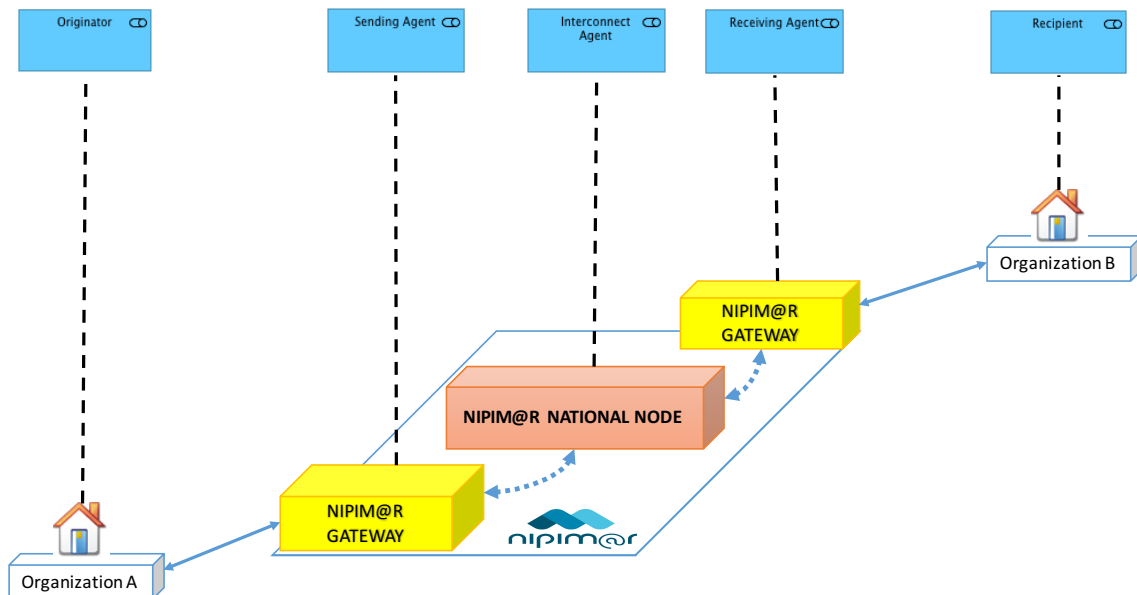


Figure 4 – Placement of Business Actors

These actors have a specific responsibility within each of the main steps of the overall message exchange process. This interaction with the process can be seen in the following sections.

2.3.1.2 High level process – Information exchange

The following figure illustrates a high-level view of the generic process for exchanging information. Presenting also the business roles and their participation.

As mentioned, this is considered a high level of the most common integration strategy used. Nevertheless, it is important to mention that other patterns in the exchange of information might already be supported, or can be in the future.

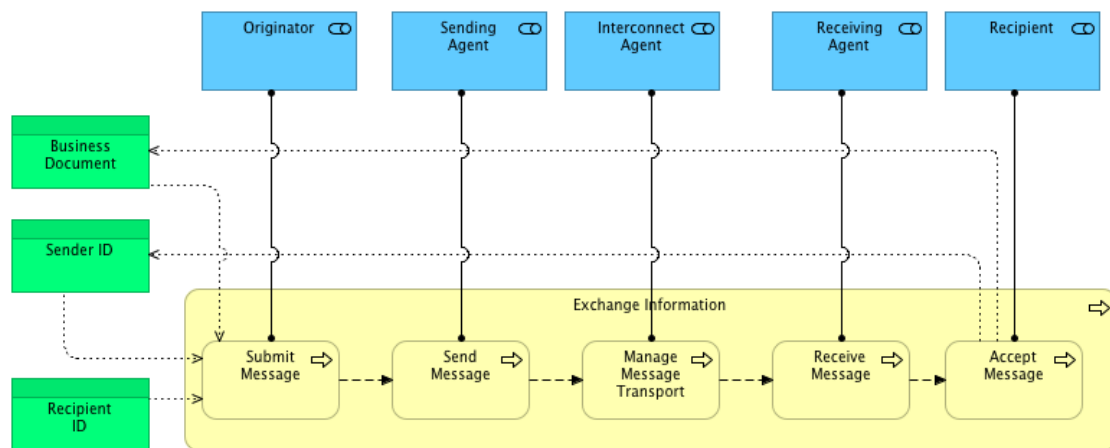


Figure 5 - High level process for information exchange

As shown in the diagram, this process can be further subdivided in five sub processes that have different acting business roles. The following table resumes each of them.

High level generic process to Exchange information	
Submit Message	The trigger for a transfer process begins with the submission of information by the partner organization that is connected to NIPIM@R (business role “Originator”).

	<p>This organization will have one or more operational systems that internally will have business needs that justify the trigger and through the usage of internal mechanisms build the necessary information to pass to the services provided by NIPIM@R to which the requests are submitted. Usually the information will be: the message itself, identification of the sender and identification of the recipient.</p> <p>This flow can be triggered by the simple act of sharing information, sending a request for which it expects to receive an answer or even provide a response to a request previously received.</p>
<p>Send Message</p>	<p>Continuing with the process, a submitted document is then received and treated by the subprocess which is the responsibility of the business actor “Sending Agent”.</p> <p>This subprocess runs a series of validations, for example verifies if the transferred information complies with the data structure and is compatible with the Message Exchange Pattern chosen.</p> <p>Carried out the necessary checks, the message is packaged with additional internal information so it can be transported and delivered to the next phase.</p>
<p>Manage Message Transport</p>	<p>This sub process, which is responsibility of the business role “Interconnect Agent”, will receive the message to transfer and do additional validations and processing regarding the finding of recipients, localization translation and necessary routing so that the message can continue the flow to the destination or destinations.</p>

Receive Message	<p>This sub process will receive the message and before delivering it to the final destination has to first extract the initial raw document that is at this phase encapsulated by an internal structure that holds information used in transport.</p> <p>Depending on the protocols and methods being used, this sub process might have to do additional transformation to comply with the destination format.</p>
Accept Message	<p>The last phase of the process in which the message is received by the final recipient and upon who resides the business decision to interpret and act on the message.</p>

Table 2 – High level generic process to Exchange information

Despite this synthesis, there are several aspects relevant for the understanding on how the process unfolds that justify a greater detail. The following sections describe each of the five sub processes with the representation of the application services that later in the Application View are mapped to their respective application.

2.3.1.3 High level sub process – Submit message

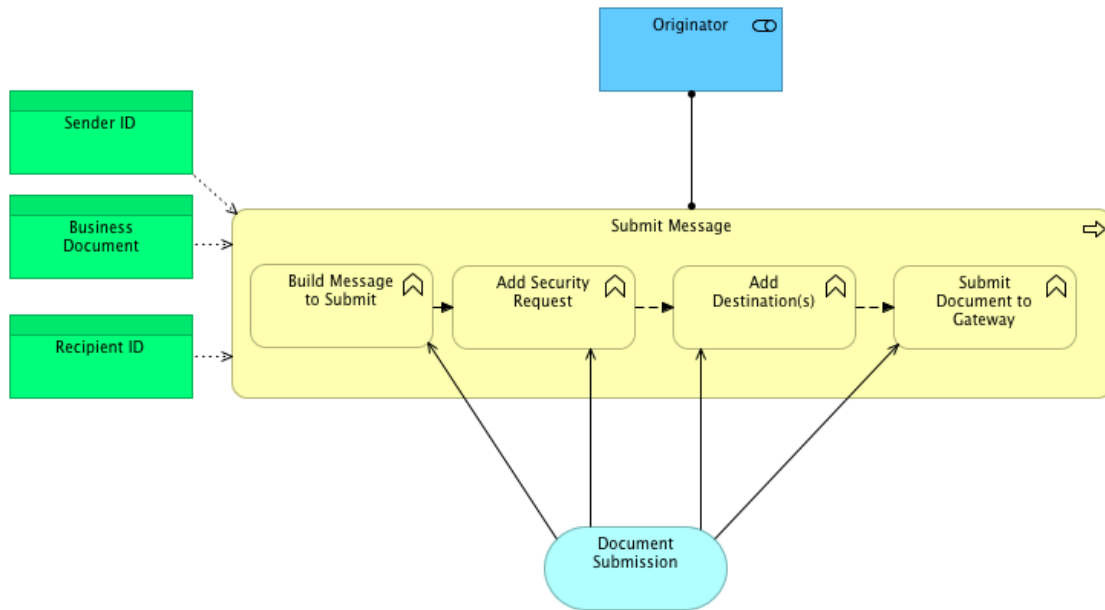


Figure 6 – Sub process “Submit Message”

Process description	
Build Message to Submit	From the need of some organizational internal business process, a message is composed with the information to be sent to the destination.
Add Security Request	To allow the transfer might be necessary to add security information, for example username/password or signature.
Add Destination(s)	Depending on the type of information, and transfer method, the destination might be known and should be added.
Submit Document to Gateway	Invocation by the originator partner organization of the services supported by NIPIM@R to transfer a message.

Table 3 – Sub process “Submit Message”

Application Service	
<div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; margin: 0 auto; background-color: #e0f7fa; display: flex; align-items: center; justify-content: center;"> <p style="margin: 0;">Document Submission</p> </div>	<p>This application service has all the necessary internal business rules of the organization that trigger the exchange of information.</p>

Table 4 – Application Service used by Sub process “Submit Message”

2.3.1.4 High level sub process – Send Message

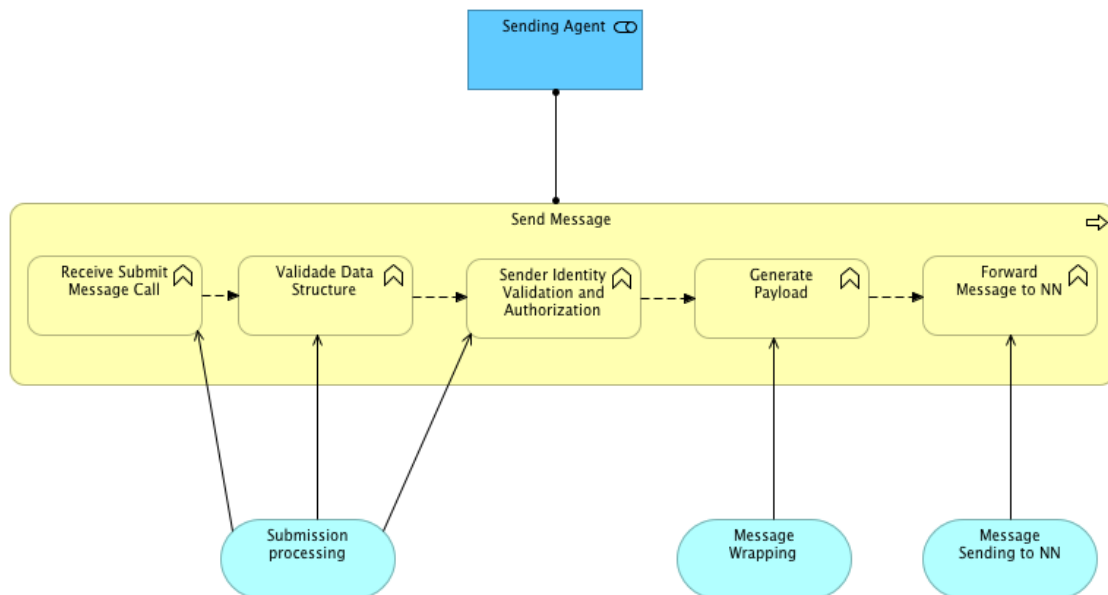


Figure 7 – Sub process “Send Message”

Process description		
Receive	Submit	Received the message in one of the access point services.
Message Call		

Validate Structure	Data	Validates the structure of the received message. For example when using NIPIM@R Web Services, is it's according with the NIPIM@R Data Model (see sections 3.2 and 3.3 for additional details).
Sender Validation and Authorization	Identity and	Verify if the sender is authorized to use the service.
Generate Payload		A payload is created that encapsulates the original document but also adds additional information regarding the destination, security, etc.
Forward Message to National Node		Send the message to the central element.

Table 5 –Sub process “Send Message”

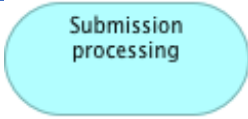
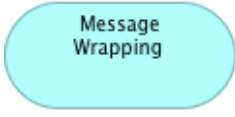
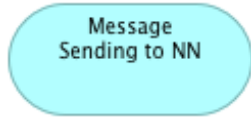
Application Service	
	This service exposes the access point where information is received from the originator organization.
	This service is used to package the original message with additional information on security and other properties that allow the end to end transport.
	Sender agent sends the generated Transport Message to the central node through a secure, reliable and asynchronous message channel

Table 6 – Application Service used by sub process “Send Message”

2.3.1.5 High level sub process – Manage Message Transport

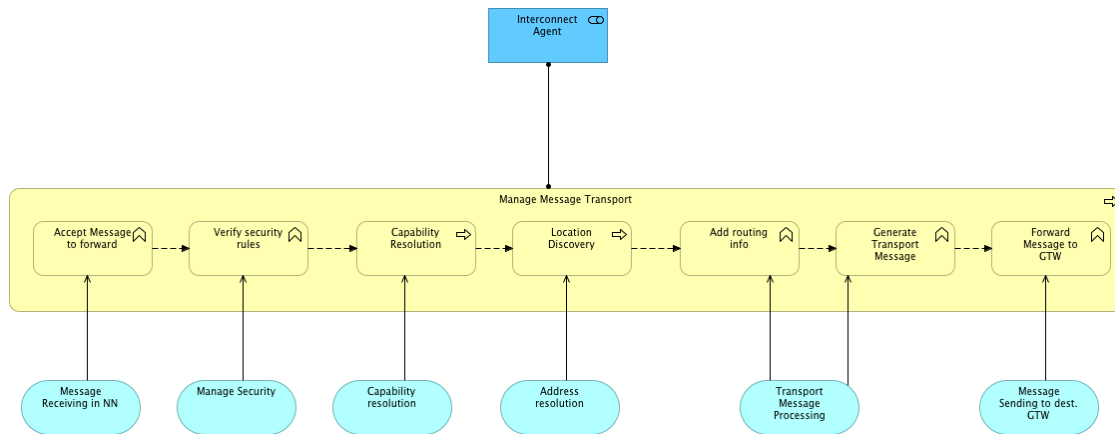


Figure 8 – Sub process “Manage Message Transport”

Process description	
Accept Message to forward	The message is received and accepted in the National Node.
Verify Security Rules	Validation rules and access policies are verified before routing the message to final destination(s).
Capability Resolution	The discovery and validation of what are the final destination capabilities and if they are compatible with the information being requested or answered.
Location Discovery	Processes the transformation of a destination recipient to the proper URL.
Add Routing Information	The necessary routing information is collected and the URL for the destination gateway is translated.

Generate Transport Message	According to configurations put in place for the particular information exchange (security measures, compression, etc.) a transport message is created.
Forward message to Gateway	Send the message to the gateway.

Table 7 –Sub process “Manage Message Transport”

Application Service	
Message Receiving in NN	The service responsible for dealing with the transport layers between the agents and the central node. Is able to “talk” the language and internal protocols put in place.
Manage Security	Handles the security services such as management of authentication and authorization.
Capability resolution	Service directly responsible for Capability Resolution Service and Capability Lookup. The service returns the metadata of the recipient agents like protocols supported.
Address resolution	This service does the necessary conversion of internal and known identifiers to addresses.
Transport Message Processing	Does the necessary transformations and adaptations to allow the correct transport to the final destination.
Message Sending to dest. GTW	This service is responsible for dealing with the transport layers between the central node and agents.

Table 8 – Application Service used by sub process “Manage Message Transport”

2.3.1.6 High level sub process – Receive Message

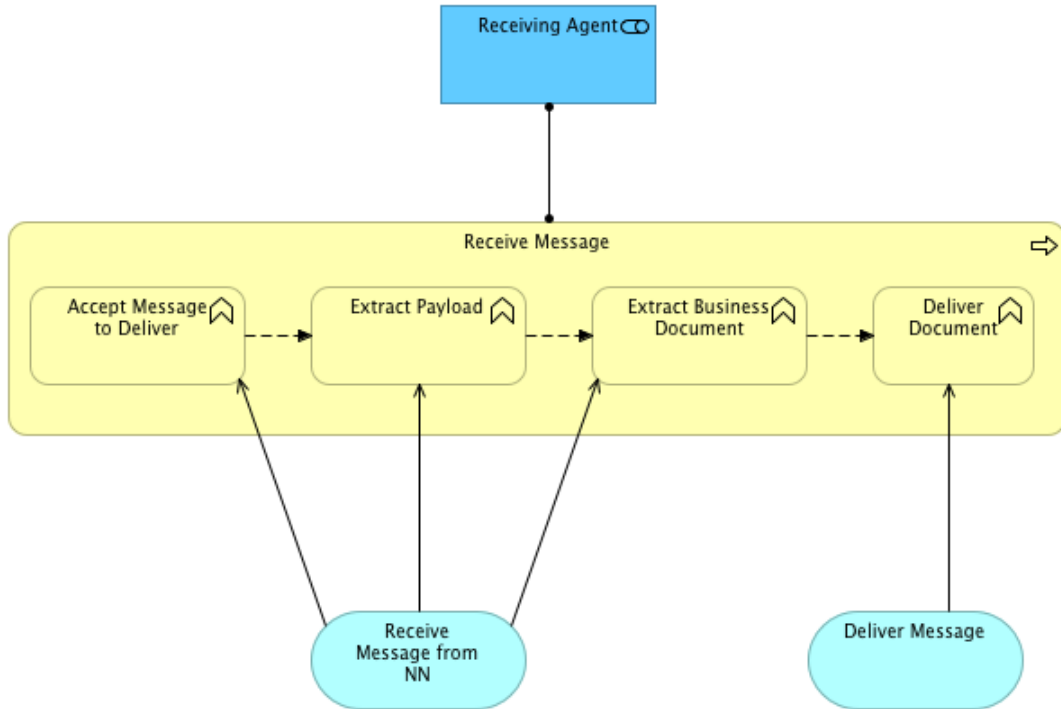


Figure 9 – Sub process “Receive Message”

Process description	
Accept Message to Deliver	Receives the message arriving in the agent.
Extract Payload	The payload is extracted from the received message.
Extract Business Document	The Business Document that was sent from the originator is extracted from the encapsulating data structures.
Deliver Document	The document is delivered to the operational system of the destination organization.

Table 9 –Sub process “Receive Message”


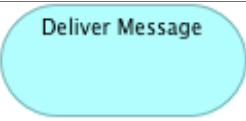
Application Service	
	Service that receives incoming messages in the channel between the agent and the central node.
	The service that upon the received message has the capability and responsibility to send to the final destination operational system.

Table 10 – Application Service used by sub process “Receive Message”

2.3.1.7 High level sub process – Accept Message

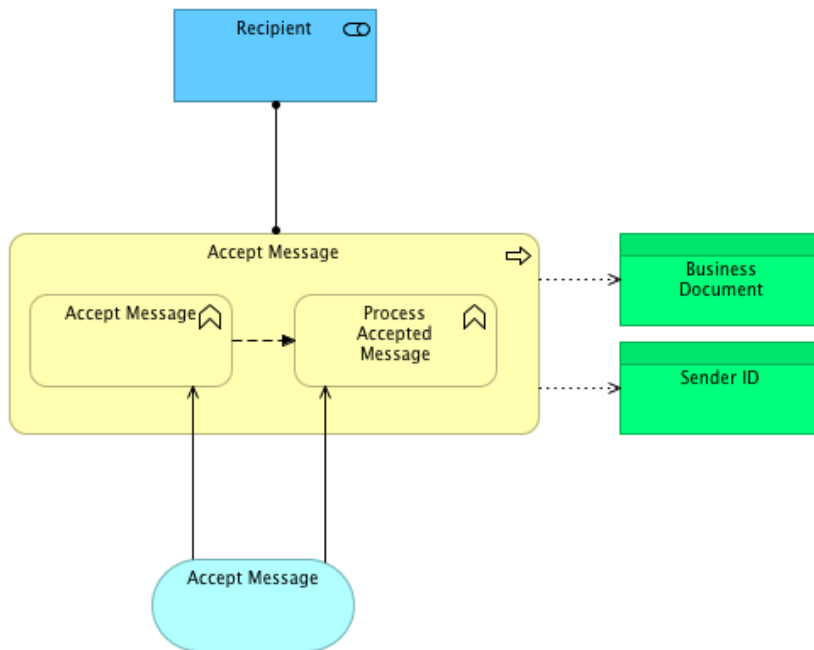


Figure 10 – Sub process “Accept Message”

Process description	
Accept Message	The original message from the originator is receive.
Process Accepted Message	The destination operational system upon receiving a message applies the designated internal business rules.

Table 11 –Sub process “Accept Message”


Application Service	
	The application services that resides in the destination operational system of the organization and who will decide what to do with the incoming message.

Table 12 – Application Service used by sub process “Accept Message”

2.3.2 Application View

Looking from an application viewpoint the services used by the functional processes can be grouped into four categories:

- NIPIM@R Core Services - Internal to NIPIM@R.
- NIPIM@R Common Services – Services available to organizations, with which they can interact.
- NIPIM@R Custom Services – Custom services to be developed in the Gateway according to specific needs.
- Organization Services – Services supplied by the organization with the objective to consume or produce information.

The following figure shows the assignment of each category in the main building blocks: NIPIM@R National Node and NIPIM@R Gateway.

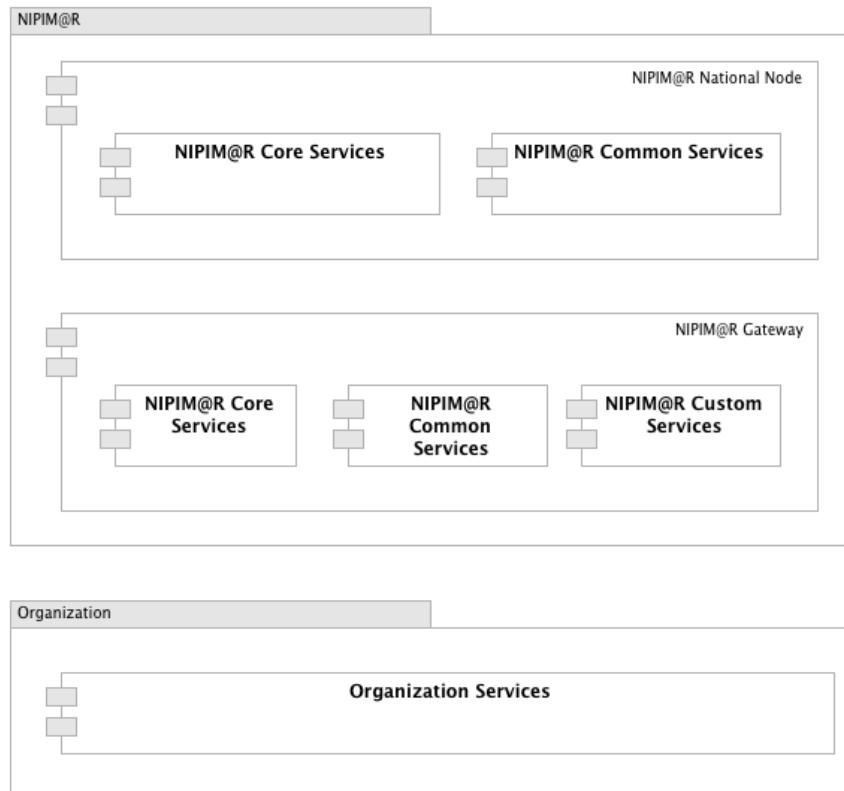


Figure 11 – Categories of Application Services

Each category classifies a set of specific services placed either in the National Node, the Gateway or in the Organization. The following figure further illustrates the decomposition and relation of the main building blocks with the services and their categories.

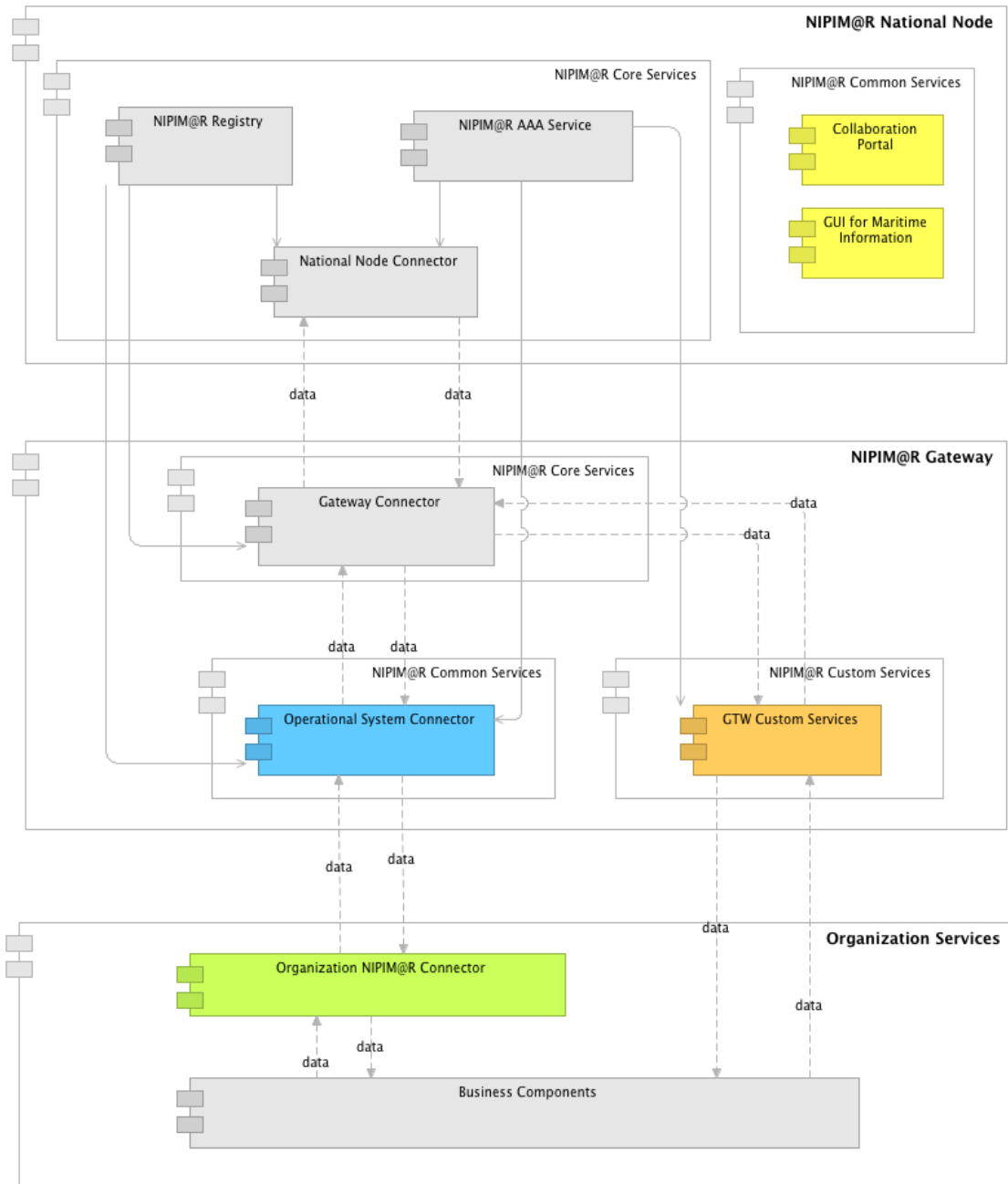


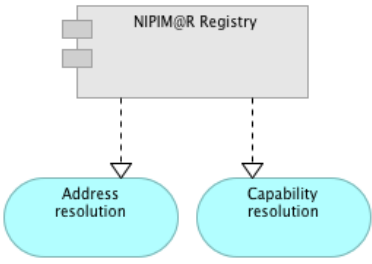
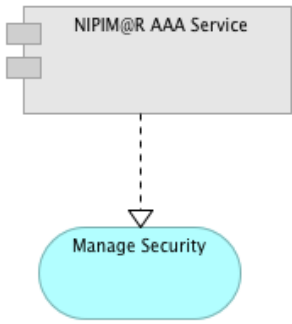
Figure 12 – NIPIM@R building blocks and application services

The following sections describe each of the applications services by their categories.

2.3.2.1 Core Application Services

Core Application Services are services and components used internally inside NIPIM@R and they are not accessible to the “outside”, but play an important role in the overall process.

The following table lists the Core Application Services and presents a brief description on their major responsibilities and roles.

Core Application Services	Description
<p>NIPIM@R Registry</p> 	<p>Provides services that support the needs for localization, name resolution and description of capabilities regarding the participating organizations. It’s used in the National Node by internal components and also in the Gateway.</p>
<p>NIPIM@R AAA Service</p> 	<p>It provides the services for registration, authentication and authorization management and enforcement. It also allows the definition of access policies that can be used to centrally filter and restrict information being transferred.</p>
<p>National Node Connector</p>	<p>This service used is the access point between the National Node and the Gateways.</p> <p>Is is responsible for the reception of data on the central node coming from a gateway and the correct routing to a destination gateway.</p>

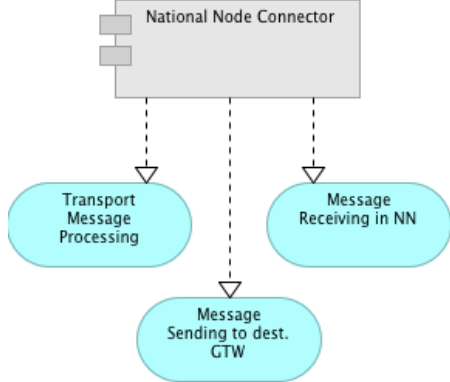
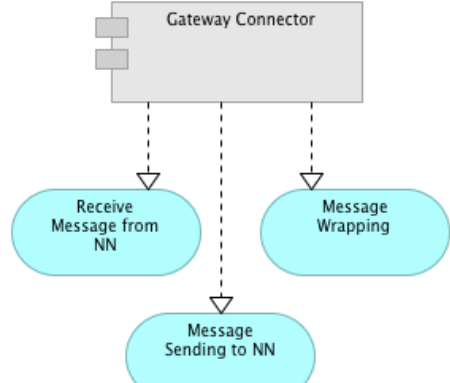

 <p>The diagram shows a grey rectangular box at the top labeled 'National Node Connector'. Three dashed arrows point downwards from this box to three light blue rounded rectangular boxes. The leftmost box is labeled 'Transport Message Processing', the middle one is 'Message Sending to dest. GTW', and the rightmost one is 'Message Receiving in NN'.</p>	<p>It expresses the process to take (store) and hand over (route and forward) business data and evidence asynchronously, securely and reliably.</p> <p>It allows:</p> <ul style="list-style-type: none"> • Several message exchange patterns • Message compression • Transmission of attachments • Error handling • Reliable messaging and Non-Repudiation Receipt • Security <p>Is linked with the Gateway Connector.</p>
<p>Gateway Connector</p>  <p>The diagram shows a grey rectangular box at the top labeled 'Gateway Connector'. Three dashed arrows point downwards from this box to three light blue rounded rectangular boxes. The leftmost box is labeled 'Receive Message from NN', the middle one is 'Message Sending to NN', and the rightmost one is 'Message Wrapping'.</p>	<p>This service used in the Gateway is the other end in the communication link between the Gateway and the National Node.</p>

Table 13 – Core Application Services

2.3.2.2 Common Application Services

The Common Application Services are application services supplied by NIPIM@R which Organizations may use.

Common Application Services		Description
Graphical User Interface for Maritime Information 	User	<p>NIPIM@R offers a Graphical User Interface to allow the viewing of a defined set of Maritime Information.</p> <p>The information available is supplied by sources already connected with NIPIM@R with whom Organizations have to agree in a Protocol to be authorized the access to this information.</p> <p>The end user access is made through a Web based application available in the National Node to authorized users. Some of the features are:</p> <ul style="list-style-type: none"> • Allows access to centralized situational awareness or distributed in real time on all relevant entities in the theatre of operations. This theatre is represented as a model on a global scale 3D real (as in common Google Earth) or a purely topographical perspective (2D). • Supports joint representations of earth, land and sea, in a single representation space. • Use line of sight calculations, the actual distance to go, as well as of land restrictions for its volumetric or position. • Each record is a iconographic form of the entity, and may be coded with colour relevant for the decision maker; • Entities are displayed in the last reported position, those with media positioning (GPS, network triangulation, etc.) are automatically updated to your position.

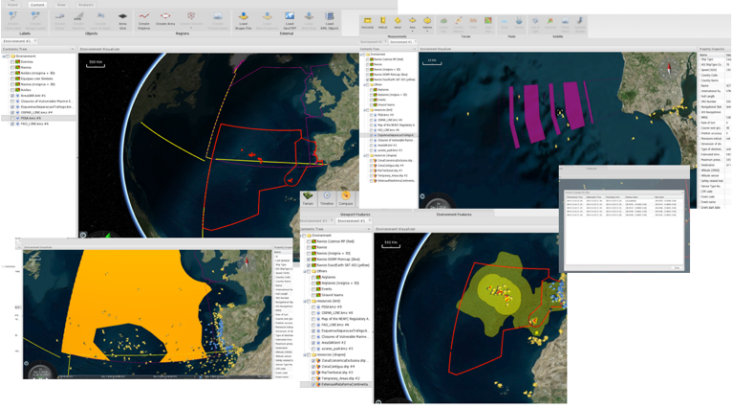
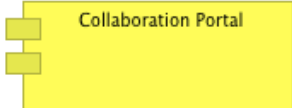
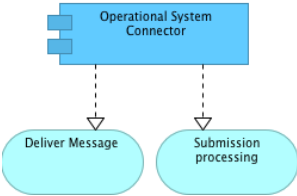
	<ul style="list-style-type: none"> • Access to ship tracks collected from various participating organizations. • Possibility to import and visualized several data formats like: KML, Shape, GeoTIFF, etc.  <p style="text-align: center;"><i>Figure 13 – Example screenshots of the GUI for Maritime Info.</i></p>
<p>Collaboration Portal</p> 	<p>A Web portal for sharing public and private information (to authorized users) related with NIPIM@R with several collaborative tools. Is one of the main vehicles for information dissemination regarding NIPIM@R.</p>
	<p>Is supplied with the NIPIM@R Gateway and already offers out-off-the-box a rich set of integration capabilities like the NIPIM@R Web Services (more details in section 3.3).</p> <p>Its usage depends on the type of Organization participation, the information exchange process chosen and type of information to share.</p> <p>Is one of the interfaces between the Gateway and the operation systems of the organization.</p>

Table 14 – Common Application Services

2.3.2.3 Custom Application Services

Custom Application Services are services that must be developed in the Gateway to support particular cases of integration.

The typical development process would be:

- Gather the requirements together with the organization, like:
 - Information to transfer;
 - Data structure;
 - Message exchange patterns to support;
 - Protocols;
 - Security;
 - Access Policies;
 - Etc.
- Develop, in the Gateway, the necessary software to orchestrate the integration process.
- Test.
- Deploy/Install.

These types of custom services are more adequate to situations where an organization has information and wants to share it but its information systems don't offer already standard interfaces to expose or to trigger the flow of information.

Following are some simple examples:

- Case 1: Organization already exchanges structured information through regular output of files to a directory.
 - Possible solution: Implement a connector in the Gateway to periodically pool a directory (thought FTP for example) and act on the information inside to send to one or more destinations.
- Case 2: Organization has information inside a Database that could be queried to produce a response to other organizations requests.

- Possible solution: Implement a connector in the Gateway that upon receiving a request from an organization (with the right permissions) makes a query through a database driver to the designated set of tables or views.
- Case 3: Organization already has capabilities to supplied streams of information (for example AIS data) to organization that subscribe it.
 - Possible solution: Implement a connector in the Gateway to conform with the subscription rules and receive the available notifications, with or without some necessary data or protocol transformations. And finally deliver it to the destinations.

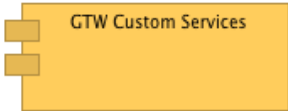
Custom Services	Application	Description
Gateway Services 	Custom	<p>These Custom Services depend of the organization where the gateway is installed and could represent specific services developed to support different message exchange patterns or some non-standard data integration capability.</p> <p>It resides is the Gateway and usually are directly connected with the Organization sources of information.</p>

Table 15 – Custom Application Services

2.3.2.4 Organization Application Services

These services reside inside the organization and represent existing sources of data or services that must be developed to participate in the exchange process with NIPIM@R.

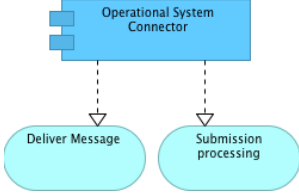

Organization Application Services		Description
Operation System Connector  <p>The diagram shows a blue rectangular box labeled 'Operational System Connector' with two small blue squares on its left side. Two dashed lines with open arrowheads point downwards from the bottom of the box to two light blue oval shapes. The left oval is labeled 'Deliver Message' and the right oval is labeled 'Submission processing'.</p>	System <p>This connector MUST be developed by the organization in the cases where it wants to interface with the existing services exposed by the Gateway either to send request or to receive the responses to previous requests.</p>	
Business Components  <p>The diagram shows a grey rectangular box labeled 'Business Components' with two small grey squares on its left side.</p>	Components <p>This generic and abstract representation defines the sources of information that exist in the organization.</p>	

Table 16 – Organization Application Services

3 Integration strategy

The integration strategy described in the following sections of this chapter represent in fact the main purpose of the document which is to provide integrators with the practical knowledge and principals to guide the integration initiative between an organization and NIPIM@R.

3.1 NIPIM@R Gateway

For the scope of this document, the presentation of this building block is the most relevant since it is the main point of contact for organizations connected to NIPIM@R.

The NIPIM@R Gateway is a component composed by software and hardware that once placed in the organizations premises where systems are intended to integrate is able to establish communications with NIPIM@R central node (the National Node).

It uses and supplies a set of integration services and interfaces that using standard's and if necessary custom connectors allow the bridging with the organizations operational systems. It supports several protocols, standards and Message Exchange Patterns (MEP) like using technics for information Pooling or other integration patterns like Request/Response, depending on the organizations particular needs when accessing or supplying data.

Additionally, the use of this Gateway component allows the transfer to it of the responsibility for compliance validation with the data structures and Message Exchange Patterns supported. It can also perform the compression of information, cryptography, data signing and other measures to ensure a safe and optimized communication.

Among other things, Gateways are responsible for sending information to the central node that in turn forwards to one or more target entities also through gateways.

The Gateway allows the implementation of additional integration services that can be tailored to the particular needs of the organization sending or receiving information. For example, an organization that already has internal services that gather and forward AIS

ship tracks in its raw format, in this case the gateway can have a custom and internal service to subscribe this information, transform it, and send of as notifications to other participating organizations that desire and are allowed to receive this tracks, hence facilitating the information exchange with minimum impact.

The Gateway is responsible for providing the necessary logical mechanisms to ensure a reliable and secure transfer of information enforcing policies and using standards.

Additionally, having very few requisites for installation it allows organizations to decide the best fit and more adequate placing in their network topologies and additional physical security measures (like firewalls, DMZ or not, etc.) they might want to use.

The two following figures exemplify possible installations scenarios with different network topologies.

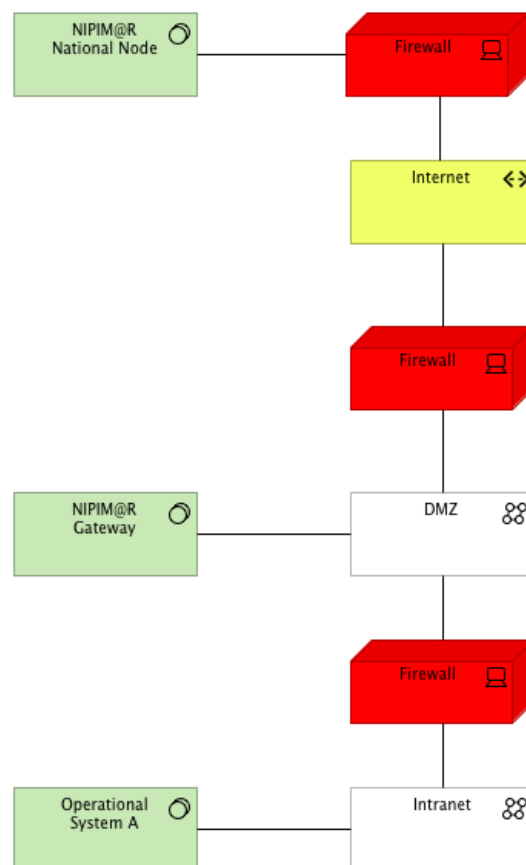


Figure 14 – Example 1 for deployment of NIPIM@R Gateway

In this example the Gateway is inside a DMZ and not in the same network as internal operational systems, this way allowing for additional security measures in between.

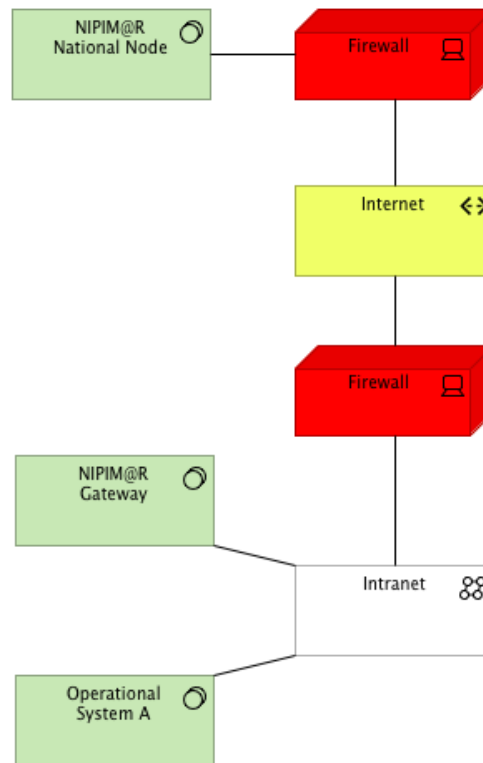


Figure 15 – Example 2 for deployment of NIPIM@R Gateway

In the last example both the Gateway and operational systems reside in the same network.

From the organizations and their software information systems perspective all integration is done directly through the NIPIM@R Gateway which acts as the single access point. Being the case of internal systems sending information, and thus accessing the Gateway available services (gateway inbound interfaces), or by being the Gateway who accesses the information systems that holds the information to exchange (in a pooling pattern) or to forward a response to information requested before (gateway outbound).

The Gateway offers several features and services that allow the integration with the organizations' information systems. These features follow in two categories: out-of-the-box services and custom services that must be developed on a request and needs basis depending on the specificities of the information and organization.

Interface/ Technology	Inbound / Outbound	Description
NIPIM@R Services	Inbound and Outbound	<p>This interface is composed by a set of Web Services that use the standard W3C Web Services stack and support several integration patterns to exchange information. These services use the NIPIM@R Data Model as the way to transfer information.</p> <p>Depending on the needs, different Message Exchange Patterns might be used.</p> <p>It's also the advisable integration technique for new developments since the services and data model will continue to evolve and be enriched moving forward to align and support the future CISE services.</p> <p>The following sections describe in more detail the features of NIPIM@R Web Services.</p>
File (SFTP; FTP)	Inbound and Outbound	The support of inbound files through SFTP or FTP is achieved with the simple pooling of a source directory (additional specific rules must be configured) and the corresponding sending as a normal unit of information through the Common Data Model to a destination organization.

		<p>Depending on specific properties regarding the files being transferred, like size, other customizations might need to be put in place.</p> <p>For outbound, again is assumed that the file being transported and delivered to the destination information system is either encapsulated by an entity of the Common Data Model and delivered as is or then is to extracted and put in a designated destination directory. Any additional needs must be customized or developed according to the organization needs.</p>
Mail	Inbound and Outbound	<p>For inbound of email through a pooling technique custom developments must be done to customize the necessary transformation rules.</p> <p>For outbound to mail boxes it can be used as an extension of typical notification services nevertheless custom developments might have to be done to customize specific data transformations and format.</p>
Information streaming pattern (AIS; Asterix; Video)	Inbound and Outbound	<p>The characteristics of information streaming flows like for example vessel position data (AIS), radar data or video stream, imposes on the architecture a different approach mainly due the information volume, constant flow of data and performance.</p> <p>In these cases, NIPIM@R already has connectors that support the receiving of AIS, Asterix and Video data in the Gateway and forward it to the</p>

		<p>Central Node where it can be consumed by authorized organizations.</p> <p>The addition of new sources is analysed to estimate possible impacts in the infrastructure and put in place the necessary measures to mitigate it.</p>
<p>Other protocols (for example REST, JMS, etc.)</p>	N/A	<p>Other protocols and integration solutions might be used since the Gateway base technologies and auxiliary services/products supply natively a large set of functionalities and support an endless number of technologies and standards.</p> <p>Following a small reference regarding the capabilities that can be used:</p> <ul style="list-style-type: none"> • Transports: HTTP, HTTPS, POP, IMAP, SMTP, JMS, AMQP, FIX, TCP, UDP, FTPS, SFTP, CIFS, MLLP and SMS • Formats & protocols: JSON, XML, SOAP 1.1, SOAP 1.2, WS-*, HTML, EDI, HL7, OAGIS, Hessian, Text, JPEG, MP4, all binary formats and CORBA/IIOP • Adapters to COTS systems: SAP BAPI & IDoc, PeopleSoft, MS Navision, IBM WebSphere MQ, Oracle AQ and MSMQ <p>When necessary, these particular integrations must be agreed between the interesting parts and if necessary additional support in the Gateway could be developed.</p>

Table 17 – Integration protocols

As stated before the placement of the Gateway and the network topology is chosen and decided by the organization where it will be installed. Nevertheless, there are two requisites that must be fulfilled to ensure the correct usage and operation of the Gateway's Hardware and Software, they are:

- Allow the network communication between the Gateway and the central National Node. Depending on the data flow it might be unidirectional or bi-directional. Meaning that in some cases an organization might only be supplying information in a Push pattern and as such no connection is begun from the National Node to the exposed services in the Gateway. This scenario is not the most usual but, if exists, it is denominated as unidirectional flow of information.
- Allow remote access to members of the NIPIM@R Operations and Support Team who are responsible for ensuring the correct operations and execution of the System. This usually is done in several ways, form example: organization supplying a VPN access to the physical machine of the Gateway; specific Firewall rules to allowing specific traffic, protocols and origin. Or other measures and technics that the organization might see fit.

Is important to mention that the physical installation and configuration of the Gateway is done in close collaboration with the organization IT teams to ensure a transparent and reliable trust model.

3.2 NIPIM@R Data Model

NIPIM@R defines a common data model based on a set of main informational entities (person, vessel, cargo, etc.) on which are provided a set of services that support the patterns of message exchange explained in the following chapters.

This data model is greatly inspired in the Common Data Model defined for the CISE initiative which was designed based on inputs from the consultation of various national and international entities working already in the exchange of information about the sea.

From which it was possible to identify a main group of informational entities and a wide range of attributes that are most common and standard across multiple sectorial systems.

Has been taken as a premise that would only be possible to support out-of-the-box a primary set of attributes, since it would not be appropriate or feasible to support all the business specifics that the participating entities might have in their data bases and systems. Thus the data model was designed in such a way that it would be possible to be extended and support the use of generic documents to be agreed between entities that exchange information.

The NIPIM@R Data Model defines seven core entities and other eleven auxiliary entities that either extend or complement the core, and together aim to supply a model a comprehensive data model.

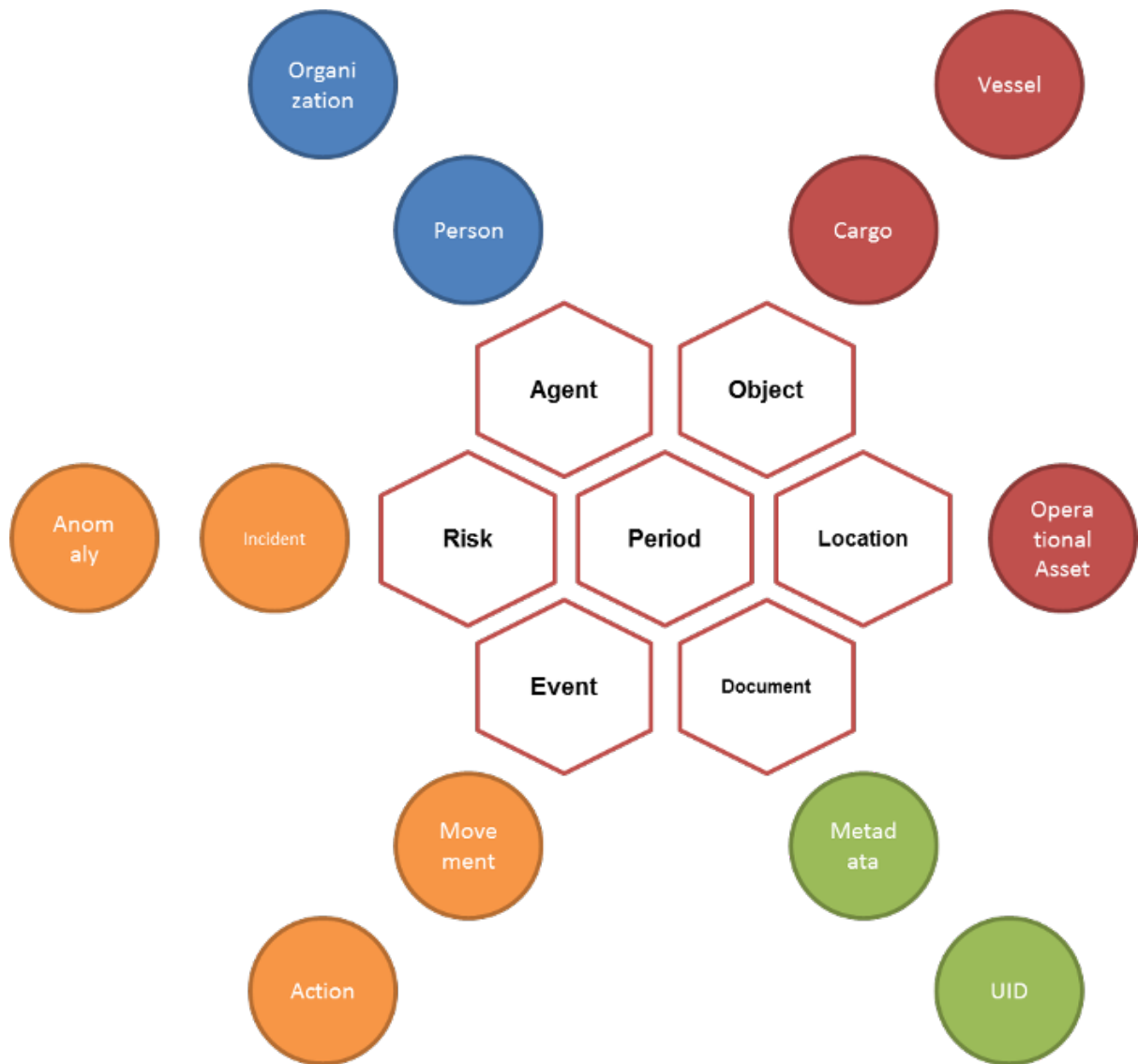


Figure 16 – Data model core entities

As represented by the previous diagram follows a brief description of the core and auxiliary entities.

Core entities:

- Agent - By definition, an Agent is an operative entity that plays a role in any Event, owns, handles or operates Objects such as Cargo or Assets, creates and exploits Documents etc. It is an entity which holds information about individual persons or organizations which are involved as actors or targets in the various

events and activities. Agent can have relationship with other agents, objects and locations. Agent can also be related to risks in different roles.

- Object – The Object entity is one of the core entities of the overall data model. It is an abstract entity (it cannot be used as such) that holds information about physical entities from the maritime domain like vehicles (vessels, aircrafts and land vehicles) and cargo. Object has relationships with Event, Agent, Document, Risk and Location. Object can also be associated with another Object.
- Location - Locations can be described in three principal ways: by using a place name, geometry or an address. The specific context will determine which method of describing a location is most appropriate. ISO 19112 defines a location as "an identifiable geographic place". With this in mind, "Eiffel Tower", "Madrid" and "California" are all locations and this is a common way of representing locations in public sector data, i.e. simply by using a recognized name. Such identifiers are common although they can be highly ambiguous as many places share the same or similar names. In addition to a simple (string) label or name for a Location, the identifier property allows defining a Location by a Uniform Resource Identifier (URI), such as a GeoNames or DBpedia URI. No cardinality constraints are placed on any property of the Location entity so as to maximize flexibility.
- Document - The Document is one of the fundamental entities of the overall data model of the information sharing environment. A Document allows tracing and exchanging information in a persistent manner in almost any possible electronic format; this information is expected to provide details on and express specific associations between other entities such as Agents, Objects, Events, Risks, Locations etc.
- Event - The Event is one of the core entities of the overall data model of the information sharing environment. It is an entity which holds information about movements, anomalies, incidents or actions which occur in the maritime domain. Event can have relationships with other events, objects, agents, documents, periods and locations. Event can also be related to risks in different

roles. Event is an abstract entity which has four sub-entities: Movement, Anomaly, Incident and Action.

- Risk - The class Risk is used to represent a more or less probable situation involving exposure to danger concerning the maritime domain. The notion of risk is usually very subjective and, in a first step, we decided to keep the definition of the class simple in order to ease its adoption. Further work could be used to detail the risk definition and introduce metrics regarding probability and severity.
- Period - Period is used to define a time interval.

Auxiliary entities:

- Person – Person is a sub entity of the more general 'Agent' entity that encompasses organizations, legal entities, groups etc. - any entity that is able to carry out actions. The data type properties of the Person class do not have any cardinality restrictions and as such all are optional.
- Organization – The class Organization is a sub-entity of an Agent. Organization represents a structured and legally recognized association of humans and material resources for some common purpose or reason for existence which goes beyond the set of people belonging to it. An organization may itself be involved as actor or target in the various events and activities. It can have relationship with other agents, objects and locations or it can be related to risks in different roles.
- Cargo – The class Cargo is a sub-entity of Object. A Cargo refers to a set of goods transported by a ship between two ports. Cargo can contain two sub-entities: Cargo Unit and Catch. It can have relationship with Document, Risk, Event, Location, and Agent.
- Vessel – The class Vessel is a sub-entity of Vehicle. A vessel refers to a ship or a boat. Vessel has the same associations and relationships than Vehicle and Object. Thus it can have relationship with Document, Risk, Event, Location, and Agent. It can also be associated with Operational Asset.

- Operational Asset - An Operational Asset is an Object (in particular means of observation or transportation, but also including associated sensors, means of communication and means of intervention such as deterrence or neutralization of threats, fire fighting, pollution containment etc.) enabling operational Actions (most often at sea or on sea shores) of the Agents mandated by public Organizations in charge of Maritime Safety and Security.
- Movement - The Movement entity is linked to Voyage. Movement can be actual (e.g. current position, heading and speed), Historical data or planned in the future and can also be expressed taking into account other entities as location, object, etc.
- Action - The Action entity may be linked to Incident, Anomaly and can also be expressed taking into account other entities as location, object, etc.
- Incident - The Incident is a sub-entity of Event. An incident refers to a particular happening, sometimes criminal but always noteworthy. Incident can have the same associations and relationships than the parent-entity Event. Thus it can have relationship with other agents, objects, documents and locations or it can be related to risks. An incident can also be associated with other(s) incident(s) (an incident can cause others for example).
- Anomaly - The class Anomaly is a sub-entity Event. An anomaly is used to characterize an unusual event which deserves to be noted or reported. Anomaly has the same associations and relationships than its parent-entity Event. Thus it can have relationship with Document, Risk, Event, Object, Period, Location, and Agent.
- Metadata - The entity provides information about the properties of the data communicated through the system, excluding the content of the data.
- Unique identifier - The Unique Identifier is a fundamental entity of the overall data model of the information sharing environment, since it will allow, as its name implies, to uniquely identify each and every single data object exchanged through the network. With this identifier it will also be possible for the operational systems to keep trace of the relationships between their data objects and those from the information sharing environment. It will be possible

to understand who and when is publishing each and every data object in the network.

These entities relate with the NIPIM@R Web Services Model in the way that through this Web Services API is possible to exchange the entities itself or the entities representing the relationships among them.

For more details on the specification of the data model is advised to consult the Annexes.

3.3 NIPIM@R Web Services Model

A service model (designated in our context as the NIPIM@R Web Services Model) is the specification of the services offered by an information provider, including the behaviour of the service and the input and output data expected by/from the service to ensure the expected behaviour.

This document is not a technical documentation of the service model but a generic introduction to its main concepts.

The service model designed for NIPIM@R is much in line with the one being defined for the EUCISE initiative. This way facilitating the future adoption and participation of Portuguese Organizations with CISE.

These services expose and allow the exchange of information based on the data model presented before. For each data entity defined the data model (i.e., each information type: Vessel, Cargo, Person, etc.), the Service Model defines a service and specific operations that support the exchange of that specific data entity using the communication patterns describe in the next section.

The NIPIM@R Web Services Model supports the information exchange using tree base patterns: pull, push, and publish/subscribe. All the information exchange patterns are asynchronous, i.e., the request of information and the response from the provider are

separate processes only connected by a correlation number, which loosely links requests and response messages.

These services are exposed through the NIPIM@R Gateway and are available out-of-the box, nevertheless organizations that want to directly interact with it must implement the respective clients and response operations in specific connector inside their operations systems.

The table below briefly describes the service operations that implement the information exchange patterns.

Data	Service	Operation	Patterns	Description
Entity	EntityService	Pull	Pull, Publish/ subscribe	This operation is invoked to request information of the type “Entity” and manage the responses. It is implemented by information providers and consumers.
		Push	Push	This operation is invoked to push information to a consumer. It is implemented by the information consumers.
		Subscribe	Push, Publish/ subscribe	This operation is invoked to subscribe or unsubscribe to a series of notifications

				It is implemented by the information providers.
--	--	--	--	---

Table 18 – Services vs Patterns

The behaviour of the service operations is also determined by the messages exchanged for each operation. The table below shows the messages accepted (as input and output) by of each operation in the information exchange process.

Data Entity	Service	Operation	Input Message	Output Message
Entity	EntityService	Pull	PullRequest	Acknowledgement
			PullResponse	
		Push	Push	Acknowledgement
		Subscribe	PullRequest	Acknowledgement
			PullResponse	

Table 19 – Services operations

The entity service model is logically structured into several main sections:

- Message metadata to identify the message type linked to a communication pattern and the correlation with other messages;
- Service Discovery to support service definition, publication and discovery activities. A service can be described and queried using a set of service profile attributes.
- Addressing describe the sender and the destination(s) of a specific message. These information is mainly used for the routing, acknowledgements and access right management;

- Payload of a message to allow the exchange of the CISE entities. The entities can be of a single type or a relation between two entities. The payload contains metadata related to the security aspects;
- Reliability profile to define the retry strategy in exchanging a message between CISE participants.

Depending on the exchange pattern and on the exchange step (transfer information, service discovery, authorization, etc.), the message structure contains only some sections. For example, the service discovery process or the acknowledgment process doesn't use the payload section. Some sections, such as addressing or message metadata are always present.

3.3.1 Message Exchange Patterns

NIPIM@R presently supports tree message exchange patterns which in essence are based on the standard patterns usually defined in Enterprise Architecture Integration called Publish / Subscribe and Request / Response.

In NIPIM@R architecture these patterns were designated Pull, Push and Publish/Subscribe.

The exchange message patterns presented are all asynchronous, i.e., the process that send information is not the same that later receives any response associated with the first sending. A strong mechanism of acknowledgments is put in place to ensure the guaranty of delivery and with the usage of message correlation identifiers attributes it allows the correct assemble of request/response in backend system and in the transfer process itself.

So regarding the patterns presently supported by the NIPIM@R Web Services, they are:

- PULL - In this pattern the Consumer request a piece of information from a Provider and later receives a response. The identity of the Provider might be known before hand or abstained dynamically from the Registry by query for available entities with specific capabilities.

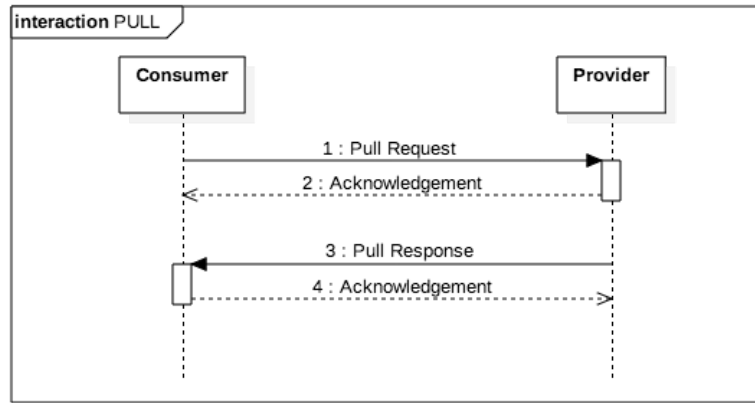


Figure 17 – Pull pattern

- PUSH - In this pattern a Consumer first has to subscribe for information that later it will receive via Notifications.

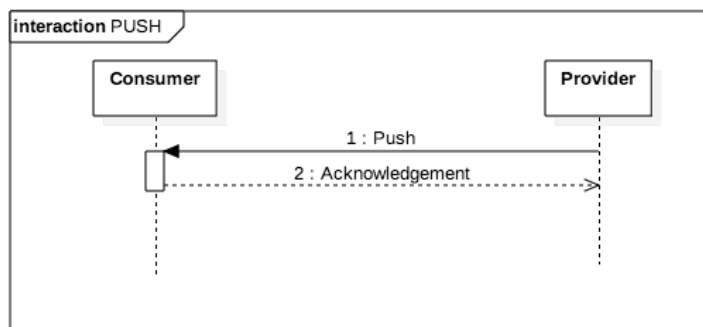


Figure 18 – Push pattern

- PUBLISH / SUBSCRIBE - In this communication pattern, the consumer subscribes to a piece of information from the NIPIM@R provider using the PullRequest operation with the subscribe PullType. When the piece of information is available in the provider, the provider notifies all the subscribers.

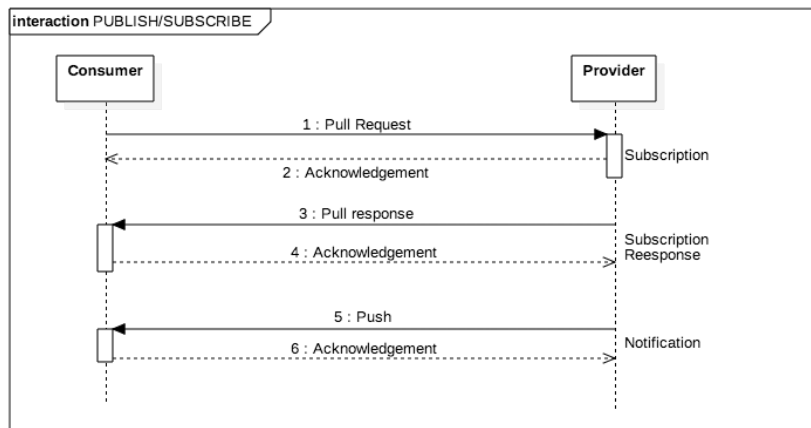


Figure 19 – Publish/Subscribe pattern

3.3.2 Message Identifiers

Message objects can contain three types of identifiers:

- MessageID: Identifier of the message. It is unique for the NIPIM@R participant who created the message.
- CorrelationID: This identifier correlates the request and response messages of/to a service (for the Pull or the Publish/Subscribe communication patterns)

3.3.3 Query base mechanism

Two query based mechanisms have been design to allow extra flexibility when using the Pull pattern. They are:

- Query-by-example mechanism

This mechanism is derived from the one envisioned by the CISE. Using this mechanism, consumers can request to a provider all the data entities that are similar to a given example.

The figure below shows an example in which the consumer sends to a provider a Vessel entity whose name is “Queen Mary” as the input of the PullRequest operation. The provider should reply with all the Vessel entities whose name is the given one.

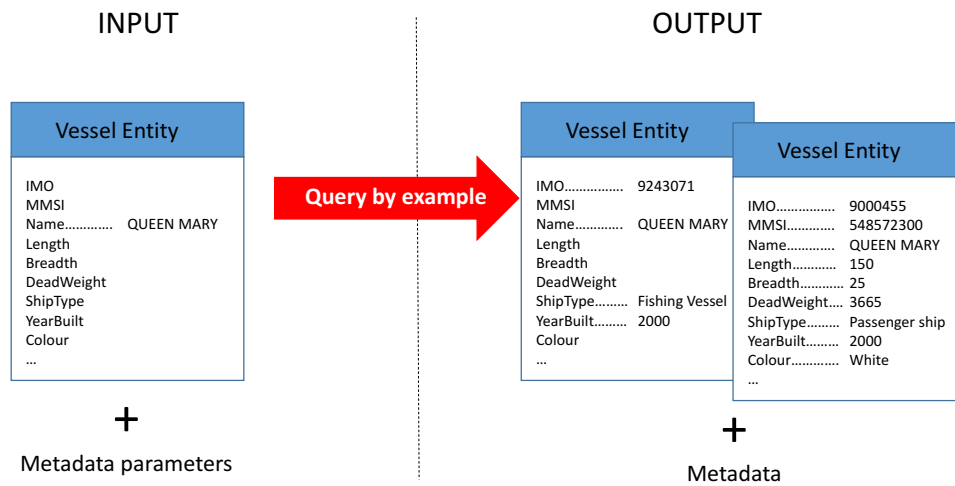


Figure 20 – Query-by-example

- Structured query mechanism

This mechanism allows a more formal but more extensible query, since complex queries can be constructed with some predefined structures and logical operands. For a consumer to define a query this way the destination must be able to understand it. So it's assumed that is the capabilities supported by the destination are well known.

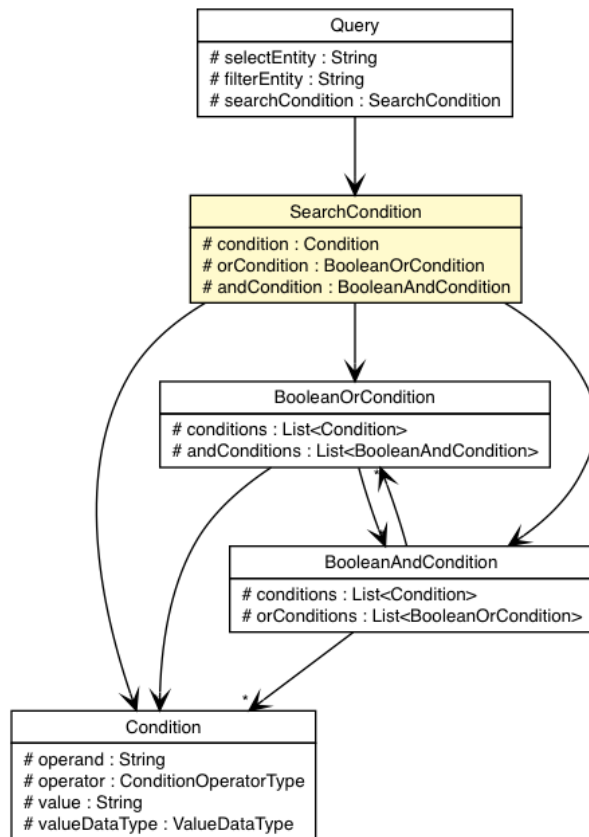


Figure 21 – Structured query

In order to limit the complexity of the service operations and facilitate its implementation, some conventions were established:

- Only one level of entity relationships. The entity payload of any message can only contain one type of data entity and the data entities directly related to it. For instance, according to the data model, a service could transmit the Vessel-Location relationship but it would not be possible to transmit the relationships Vessel-Location and Vessel-Cargo with a single service.
- Best match. The providers should deliver a PullResponse message containing data entities that are the most similar to the requested query-by-example entity contained in the corresponding PullRequest message. ServiceCapability parameters are required to indicate which kind of response (QueryByExampleType) is required/delivered, i.e., exact or best match.

- Full vs. partial response. Open queries can result in a high number of responses, or in large responses, which could slow down (or even block) the provider's systems or the NIPIM@R network. In order to avoid this problem, some metadata within the service capabilities is also required to indicate the maximum number of responses (MaxEntitiesPerMsg).

3.4 Security model

Regarding the security model it is important to differentiate the internal measures put in place by NIPIM@R regarding the link between the Gateway and the National Node (A), from the link between the Gateway and the organizations operational systems (B).

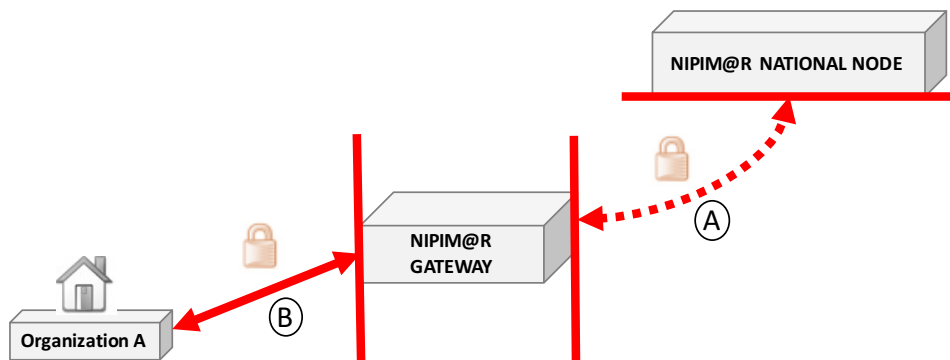


Figure 22 – Overview of the security boundaries

3.4.1 NIPIM@R Gateway to/from NIPIM@R National Node

The physical and logical security between the National Node and the Gateway will not be detailed in this document but the security, reliability and confidentiality is assured by a set of measures that range from authentication and authorization policies, cypher, secure communication channels and physical measures like firewalls.

3.4.2 NIPIM@R Gateway to/from Operational Systems

As stated before the Gateway is the access point for the organization internal systems either to send information, receive or both. The security measures and requirements to

implement will vary from organization to organization and will also be influenced by the type and needs of integration.

These physical and logical measures should be decided by the organization IT Team and should take in consideration the deployment scenario and the security model.

4 References

- The general eSens building blocks presentation: <http://www.esens.eu/technical-solutions/>
- Connecting Europe Facility (CEF) – Building Block: https://joinup.ec.europa.eu/community/cef/og_page/catalogue-building-blocks
- eSens Wiki: <http://wiki.ds.unipi.gr/display/ESENS/Overview>
- CIPA e-Delivery on JoinUp: <https://joinup.ec.europa.eu/software/cipaedelivery/description>
- Animation to present a simple message exchange with e-Delivery: http://prezi.com/z_j0-kkzvm3-/cef-edelivery-dsi/
- White Paper on Integrating Maritime Surveillance: the Implementation of the Common Information Sharing Environment: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_mare_002_cise_en.pdf
- JoinUp collaborative environment for CISE: https://joinup.ec.europa.eu/software/digit_cise/home

Appendix 1 – Data model specifications (XSD)

The XSD specifications for the NIPIM@R Data Model are supplied in an external compressed file (ZIP) attached with this document.

Appendix 2 – Information services specifications (WSDL)

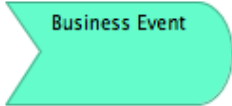
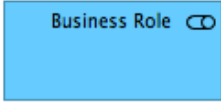
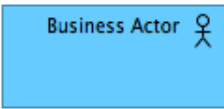


The services specifications (WSDL's) for the NIPIM@R Web Services are supplied in an external compressed file (ZIP) attached with this document.

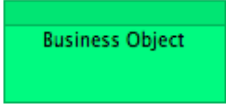
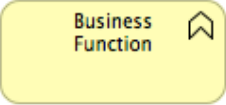
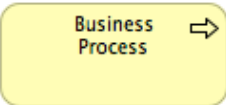





Appendix 3 – Archimate Quick Reference Guide

To help clarify the reading of this document it is important to present a quick overview of the notation used to describe several concepts and architectural views along the document.

Several architectural views present in this document are described using the ArchiMate® notation.

The following table presents a summary of the main figures used and their meaning.

Notation	Description
	A business event is defined as something that happens (internally or externally) and influences behaviour (business process, business function, business interaction).
	A business role is defined as a named specific behaviour of a business actor participating in a given context. The actor performs the behaviour of the role.
	A business actor is defined as an entity that performs behaviour in an organisation such as business processes or functions.
	An application component is defined as a modular, deployable, and replaceable part of a system that encapsulates its contents and exposes its functionality through a set of interfaces.
	An application service is defined as an externally visible unit of functionality, provided by one or more components, exposed through well-defined interfaces, and meaningful to the environment.

	<p>A business object is defined as a unit of information that has relevance from a business perspective.</p>
	<p>A business function describes internal behaviour performed by a business role that is required to produce a set of products and services. It is performed by a single role within an organisation.</p>
	<p>A business process is defined as a unit of internal behaviour or collection of causally-related units of internal behaviour intended to produce a defined set of products and services.</p>
	<p>The realization relationship links a logical entity with a more concrete entity that realizes it.</p>
	<p>The assignment relationship links active elements (e.g., business roles or application components) with units of behavior that are performed by them, or business actors with business roles that are fulfilled by them.</p>
	<p>The used by relationship models the use of services by processes, functions, or interactions and the access to interfaces by roles, components, or collaborations.</p>
	<p>The access relationship indicates that a process, function, interaction, service, or event "does something" with a (business or data) object.</p>
	<p>The flow relationship describes the exchange or transfer of information or value between processes, function, interactions, and events.</p>