EUROPEAN COMMISSION

EUROPEAN MARITIME SAFETY AGENCY

Cais Do Sodré 1249-206 Lisbon, Portugal

SafeSeaNet System Design Document

NSW Prototype

Document version: 1.91

Document release date: July 2015

Document Approval

	NAME	DATE	SIGNATURE
Prepared by:	H. Routis A. Sergouniotis C. Trigonis	03/07/2015	
Checked by:	A. Argyropoulos	07/07/2015	
Quality control by:	N. Karioti	07/07/2015	
Approved by:	G. Carayannis	07/07/2015	

Distribution List

COMPANY	NAME	FUNCTION	FOR INFO / APPROVAL
EMSA	Duchesne Philippe		
EMSA	Abela Carmelo		
Member States			
SSN central system contractor			

Change control History

VERSION	DATE	AUTHOR	DESCRIPTION
0.10	07 Aug 2013	Intrasoft International	First Draft submitted to internal QA for Review.
0.90	12 Aug 2013	Intrasoft International	Submitted to EMSA for Review.
1.00	05 Sep 2013	Intrasoft International	Incorporated EMSA review comments.
1.10	20 Sep 2013	Intrasoft International	Final version covering the Data Capture process.
1.20	18 Oct 2013	Intrasoft International	Updated to define the Consult Acknowledgment related business process and use case, and define the SSN Central required domain and database upgrades.
1.30	29 Nov 2013	Intrasoft International	Incorporated EMSA review comments
1.40	16 Dec 2013	Intrasoft International	Updated according to SDD review teleconference on 09/12/2013. Submitted to EMSA for acceptance.

1.50	17 Feb 2014	Intrasoft International	Updated to incorporate the additional functionalities for the NSW prototype based on the SC#07 evolutive maintenance task.
1.55	14 Mar 2014	Intrasoft International	Updated according to EMSA review comments. Submitted to EMSA for acceptance
1.60	23 May 2014	Intrasoft International	Updated to incorporate design changes part of SC#09. Submitted to EMSA for review
1.65	05 Jun 2014	Intrasoft International	Updated to incorporate EMSA review comments.
1.70	03.07.2014	Intrasoft International	Updated to incorporate further EMSA review comments. Submitted for acceptance.
1.75	15.07.2014	Intrasoft International	Updated to merge Cargo Items and DPG Items. Section 5.1 and annex C. Submitted for acceptance.
1.80	26.08.2014	Intrasoft International	Incorporated final EMSA comments in the context of SC#09.
1.85	01.10.2014	Intrasoft International	Updated in the context of SC#11 NSW prototype V3.
1.86	02.10.2014	Intrasoft International	Incorporated EMSA review comments.
1.87	19.10.2014	Intrasoft International	Updated to process further EMSA review comments and according to the v1.86 review teleconference.
1.88	22.10.2014	Intrasoft International	Incorporated EMSA review comments to v1.87.
1.90	08.04.2015	Intrasoft International	Updated in the context of SC#09 evolutive maintenance #01
1.91	07.07.2015	Intrasoft International	Incorporated EMSA review comments to v1.91

Table of Contents

1 Introduction

1.1 Purpose

This document defines the National Single Window (NSW) system design in the scope of SC#07, SC#09 (including evolutive maintenance Nr.01) and SC#11 implementing FC 11/EMSA/OP/08/2011 “SafeSeaNet enhancements for the further improvements of SSN v2 in light of the MS decisions in SSN 15, 16, 17 of HLSG7” work package 3 – IMP demonstration project.

1.2 Scope

This document is the *Design Approach Document* for the NSW system. The purpose of this document is to present a comprehensive architectural overview / the technical details of the NSW system components and more specifically:

- The definition of system architecture, components, classes, their attributes and methods that will implement the requested functionality.
- The database system design including the definition of database tables, table relations, table fields.
- It shall be noted that the graphical interface design of the NSW web applications is defined in the corresponding GIDD.

It presents a number of different architectural views to depict different aspects of the system. It is intended to capture and convey the significant architectural decisions which have been made on the system.

The primary intended audience of this document are system designers and system builders. The document intents to provide the members of the IMP demonstration project a unified view of the technical details of the system design to be followed during the development of the respective application. The document may need to be updated later to incorporate possible changes during development.

1.3 Reference documents

Id	Reference	Title	Version
R1	RUP Formal Resources Version 1.2	Rational Unified Process Formal Resources based on RUP Version: 2003.06.13	1.2
R2	N/A	Intrasoft International Quality Assurance Book	2.10
R3	N/A	Business Process Modelling Notation (BPMN)	1.2
R4	ISO/PAS 28005-1 :2012(E)	Ships and marine technology — Electronic port clearance (EPC) — Part 1: Message structures — Implementation of a maritime single window system	N/A

Id	Reference	Title	Version
R5	ISO 28005-2:2011(E)	Security management systems for the supply chain — Electronic port clearance (EPC) — Part 2: Core data elements	N/A
R6	SSN-SDD	SSN EIS System design Document	1.00
R7	System Application Technical Landscape	EMSA Internal System and Application Technical Landscape	20 from 06/02/2013
R8	IMP-Demo-SRS	NSW System Requirements Specifications	1.12
R9	IMP SSN-objectives and technical specifications	SC#09 under FMC EMSA 11/EMSA/OP/08/2011	1
R10	NSW prototype V3-objectives and technical specifications	SC#11 under FMC EMSA 11/EMSA/OP/08/2011	19/06/2014
R11	Master file-NSW prototype	NSW prototype data groups and elements definition.	15/04/2015

Table 1-1: Reference Documents

1.4 Abbreviations and acronyms

A list of the principal abbreviations and acronyms used in the document is provided here for a better understanding of this document.

Abbreviation	Definition
AIE	Authority Information Exchange
BPMN	Business Process Modelling Notation
CDI	Contexts and Dependency Injection
CRG	Common Reporting Gateway
EMSA	European Maritime Safety Agency
EPC	Electronic Port Clearance
FAL	Facilitation, IMO's Facilitation Committee and standard forms defined in the FAL Convention
GIS	Geographic Information System
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over SSL
ID	Identification number
IMO	International Maritime Organisation
IMP	Integrated Maritime Policy

Abbreviation	Definition
II	INTRASOFT International
ISPS	International Ship and Port Facility Security code
MMSI	Maritime Mobile Service Identity
MS	Member State
N/A	Not Applicable or Not Available
NSW	National Single Window
REST	REpresentational State Transfer technology
RUP	Rational Unified Process
QoS	Quality of Service
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SSN	SafeSeaNet
SSO	Single Sign-On
TR	Table Reference
UML	Unified Modelling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WADL	Web Application Description Language. It describes XML over HTTP interfaces
WSDL	Web Services Description Language
XML	eXtensible Markup Language
XSD	XML Schema Definition Language
XSL-FO	Extensible Stylesheet Language Formatting Objects
XSLT	Extensible Stylesheet Language Transformations

Table 1-2: Abbreviations and Acronyms

2 Architectural Goals and Constraints

This section describes the software requirements and objectives that have some significant impact on the architecture.

Given that NSW application shall integrate information from different sources and perform systematic correlation of real time information, its architecture is based on EAI approach and EIP design patterns.

The NSW architecture respects the following architectural principles and technologies:

2.1 Service-Oriented Architecture (SOA)

A SOA is an architecture principle that is based on the key concept of services. A service, in its simplest form, consists of an interface and an implementation. SOA defines software applications in terms of discrete services, which are implemented using service components that can be used to perform business activities for a given business process.

One perceived value of SOA is that it provides a powerful framework for matching needs and capabilities and for combining capabilities to address those needs by leveraging other capabilities. One capability may be repurposed across a multitude of needs.

SOA is a "view" of architecture that focuses on services as the action boundaries between the needs and capabilities in a manner conducive to service discovery and repurposing.

2.2 Java EE features

2.2.1 Contexts and Dependency Injection (CDI)

Contexts and Dependency Injection (CDI) for the Java EE platform is one of several Java EE 6 features that help to knit together the web tier and the transactional tier of the Java EE platform.

CDI is a set of services that, used together, make it easy for developers to use enterprise beans along with JavaServer Faces technology in web applications. Designed for use with stateful objects, CDI also has many broader uses, allowing developers a great deal of flexibility to integrate various kinds of components in a loosely coupled but typesafe way.

CDI is specified by JSR 299, formerly known as Web Beans. Related specifications that CDI uses include the following:

- JSR 330, Dependency Injection for Java
- The Managed Beans specification, which is an offshoot of the Java EE 6 platform specification (JSR 316)

The most fundamental services provided by CDI are as follows:

- Contexts: The ability to bind the lifecycle and interactions of stateful components to well-defined but extensible lifecycle contexts
- Dependency injection: The ability to inject components into an application in a typesafe way, including the ability to choose at deployment time which implementation of a particular interface to inject

In addition, CDI provides the following services:

- Integration with the Expression Language (EL), which allows any component to be used directly within a JavaServer Faces page or a JavaServer Pages page
- The ability to decorate injected components
- The ability to associate interceptors with components using typesafe interceptor bindings
- An event-notification model
- A web conversation scope in addition to the three standard scopes (request, session, and application) defined by the Java Servlet specification
- A complete Service Provider Interface (SPI) that allows third-party frameworks to integrate cleanly in the Java EE 6 environment

A major theme of CDI is loose coupling. CDI does the following:

- Decouples the server and the client by means of well-defined types and qualifiers, so that the server implementation may vary
- Decouples the lifecycles of collaborating components by doing the following:
- Making components contextual, with automatic lifecycle management
- Allowing stateful components to interact like services, purely by message passing
- Completely decouples message producers from consumers, by means of events
- Decouples orthogonal concerns by means of Java EE interceptors

Along with loose coupling, CDI provides strong typing by

- Eliminating lookup using string-based names for wiring and correlations, so that the compiler will detect typing errors
- Allowing the use of declarative Java annotations to specify everything, largely eliminating the need for XML deployment descriptors, and making it easy to provide tools that introspect the code and understand the dependency structure at development time.

Weld, a CDI Reference Implementation (RI), shall be used for the NSW implementation.

Weld provides a complete SPI, allowing Java EE containers such as JBoss AS, GlassFish and WebLogic to use Weld as their built-in CDI implementation. Weld also runs in servlet engines like Tomcat and Jetty, or even in a plain Java SE environment.

2.2.2 Java Persistence API

The Java Persistence API (JPA) is a Java standards-based solution for persistence. Persistence uses an object/relational mapping approach to bridge the gap between an object-oriented model and a relational database. The Java Persistence API can also be used in Java SE applications, outside of the Java EE environment. Java Persistence consists of the following areas:

- The Java Persistence API
- The query language
- Object/relational mapping metadata

The Java EE 6 platform requires Java Persistence API 2.0.

JPA 2.0 (JSR 317) shall be used. The main features included in this update are:

- expanded object-relational mapping functionality

    - support for collections of embedded objects, linked in the ORM with a many-to-one relationship
    - multiple levels of embedded objects
    - ordered lists
    - combinations of access types
- criteria query API
- standardization of query 'hints'
- standardization of additional metadata to support DDL generation
- support for validation

EclipseLink JPA shall be used for the implementation of JPA specification.

2.3 Open Source Frameworks

2.3.1 Spring framework

Spring Framework is a Java platform that provides comprehensive infrastructure support for developing Java applications. Spring facilitates the applications building from "plain old Java objects" (POJOs) and to apply enterprise services non-invasively to POJOs. This capability applies to the Java SE programming model and to full and partial Java EE.

Some of the Spring platform advantages are:

- Make a Java method execute in a transaction without having to deal with transaction APIs.
- Make a local Java method a remote procedure without having to deal with remote APIs.
- Make a local Java method a message handler without having to deal with JMS APIs.

The Spring Framework consists of features organized into about 20 modules. These modules are grouped into Core Container, Data Access/Integration, Web, AOP (Aspect Oriented Programming), Instrumentation, and Test, as shown in the following diagram.

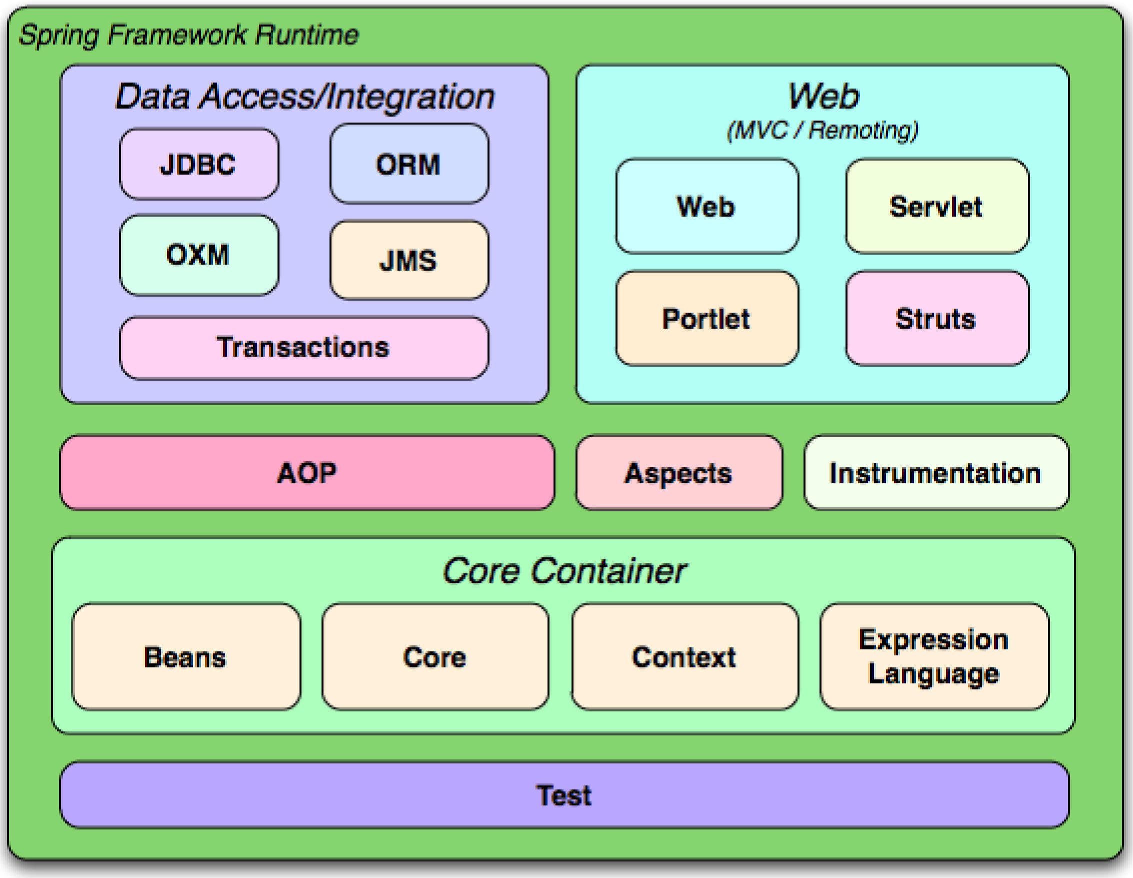


Figure 2-1. Spring Framework Runtime.

Key technologies (Java EE) provided by Spring Framework on Presentation layer include the following:

- Java Servlet
- JavaServer Faces
- Web application internationalization and localization
- Security
- MVC
- Comprehensive REST support

Spring Web Flow

Spring Web Flow is a Spring MVC extension that allows implementing the "flows" of a web application. A flow encapsulates a sequence of steps that guide a user through the execution of some business task. It spans multiple HTTP requests, has state, deals with transactional data, is reusable, and may be dynamic and long-running in nature.

The sweet spot for Spring Web Flow are stateful web applications with controlled navigation such as checking in for a flight, applying for a loan, shopping cart checkout, or even adding a confirmation step to a form. What these scenarios have in common is one or more of the following traits:

- There is a clear start and an end point.
- The user must go through a set of screens in a specific order.
- The changes are not finalized until the last step.
- Once complete it shouldn't be possible to repeat a transaction accidentally.

Spring Web Flow provides a declarative flow definition language for authoring flows on a higher level of abstraction. It allows it to be integrated into a wide range of applications without any changes (to the flow programming model) including Spring MVC, JSF, and even Portlet web applications.

Spring Framework version 3.2.x and Spring Web Flow version 2.3.x shall be used for NSW web applications implementation (Presentation layer).

2.3.2 ESAPI (The OWASP Enterprise Security API)

ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications. The ESAPI libraries are designed to make it easier for programmers to retrofit security into existing applications. The ESAPI libraries also serve as a solid foundation for new development.

Allowing for language-specific differences, all OWASP ESAPI versions have the same basic design:

- There is a set of security control interfaces. They define for example types of parameters that are passed to types of security controls.
- There is a reference implementation for each security control. The logic is not organization-specific and the logic is not application-specific. An example: string-based input validation.
- There are optionally your own implementations for each security control. There may be application logic contained in these classes which may be developed by or for your organization. An example: enterprise authentication.

2.4 Web features

2.4.1 HTML5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. Its core aims have been to improve the language with support for the latest multimedia while keeping it easily readable by humans and consistently understood by computers and devices (web browsers, parsers, etc.). HTML5 is intended to subsume not only HTML 4, but also XHTML 1 and DOM Level 2 HTML.

Following its immediate predecessors HTML 4.01 and XHTML 1.1, HTML5 is a response to the observation that the HTML and XHTML in common use on the World Wide Web are a mixture of features introduced by various specifications, along with those introduced by software products such as web browsers, those established by common practice, and the many syntax errors in existing web documents. It is also an attempt to define a single markup language that can be written in either HTML or XHTML syntax. It includes detailed processing models to encourage more interoperable implementations; it extends, improves and rationalises the markup available for documents, and introduces markup and application programming interfaces (APIs) for complex web applications. For the same reasons, HTML5 is also a potential candidate for cross-platform mobile applications. Many features of HTML5 have been built with the consideration of being able to run on low-powered devices such as smartphones and tablets.

In particular, HTML5 adds many new syntactic features as the new <video>, <audio> and <canvas> elements, as well as the integration of scalable vector graphics (SVG) content (that replaces the uses of generic <object> tags) and MathML for mathematical formulas. These features are designed to make it easy to include and handle multimedia and graphical content on the web without having to resort to proprietary plugins and APIs. Other new elements, such as <section>, <article>, <header> and <nav>, are designed to enrich the semantic content of documents. New attributes have been introduced for the same purpose, while some elements and attributes have been removed. Some elements, such as <a>, <cite> and <menu> have been changed, redefined or standardized. The APIs and Document Object Model (DOM) are no longer afterthoughts, but are fundamental parts of the HTML5 specification. HTML5 also defines in some detail the required processing for invalid documents so that syntax errors will be treated uniformly by all conforming browsers and other user agents.

2.4.2 JavaServer Faces

JavaServer Faces (JSF) is a user interface (UI) framework for Java web applications. It is designed to significantly ease the burden of writing and maintaining applications that run on a Java application server and render their UIs back to a target client. JSF provides ease-of-use in the following ways:

- Makes it easy to construct a UI from a set of reusable UI components
- Simplifies migration of application data to and from the UI
- Helps manage UI state across server requests
- Provides a simple model for wiring client-generated events to server-side application code
- Allows custom UI components to be easily built and re-used

Most importantly, JSF establishes standards which are designed to be leveraged by tools to provide a developer experience which is accessible to a wide variety of developer types, ranging from corporate developers to systems programmers. A "corporate developer" is characterized as an individual who is proficient in writing procedural code and business logic, but is not necessarily skilled in object-oriented programming. A "systems programmer" understands object-oriented fundamentals, including abstraction and designing for re-use. A corporate developer typically relies on tools for development, while a system programmer may define his or her tool as a text editor for writing code.

Therefore, JSF is designed to be tooled, but also exposes the framework and programming model as APIs so that it can be used outside of tools, as is sometimes required by systems programmers.

2.4.3 XLS-FO and XSLT

XSL-FO stands for Extensible Stylesheet Language Formatting Objects. XSL-FO is a W3C specification for formatting XML data for output to screen, paper or other media. In the IMP demonstrator project it is primarily used as the basis for the production of the XLS and PDF file outputs.

The implementation for the generation of the PDF output is using the Apache FOP for the creation of the XSL-FO templates.

XSLT (Extensible Stylesheet Language Transformations) is finally used to transform the EPC XML messages in XSL-FO.

2.5 Single Sign-On

Single Sign-On (SSO) is the ability to require a user to sign on to an application only once and gain access to many different application components, even though these components may have their own authentication schemes. Single sign-on enables users to login securely to all their applications with just one identity authentication between Web applications running in a WebLogic Server domain

2.5.1 Security Providers

Security providers are modular components that handle specific aspects of security, such as authentication and authorization. The WebLogic and Tomcat Security Service’s flexible infrastructure also allows security vendors to write their own custom security providers. WebLogic and Tomcat security providers and custom security providers can be mixed and matched to create unique security solutions, allowing organizations to take advantage of new technology advances in some areas while retaining proven methods in others.

The following types of security providers are used by SSO configuration:

- **Authentication**—Authentication is the process whereby the identity of users or system processes are proved or verified. Authentication also involves remembering, transporting, and making identity information available to various components of a system when that information is needed. Authentication providers supported by the WebLogic Security Service supply the following types of authentication:
    - Username and password authentication
    - Certificate-based authentication directly with WebLogic Server and Tomcat Server.
    - HTTP certificate-based authentication proxied through an external Web server.

  An RDBMS Authentication provider is a username/password based Authentication provider that uses a relational database as its data store for user, password, and group information. Read-only SQL Authenticator uses a SQL database and allows only read access to the database.

- **Identity Assertion** (applicable only for WebLogic Server)—An Authentication provider that performs perimeter authentication—a special type of authentication using tokens—is called an Identity Assertion provider. Identity assertion involves establishing a client's identity through the use of client-supplied tokens that may exist outside of the request. Thus, the function of an Identity Assertion provider is to validate and map a token to a username. Once this mapping is complete, an Authentication provider’s LoginModule can be used to convert the username to a principal (an authenticated user, group, or system process).

.

2.5.2 SAML-Based Single Sign-On

Security Assertion Markup Language (SAML) enables cross-platform authentication between Web applications or Web Services running in an Application Server domain and Web browsers or other HTTP clients. WebLogic and Tomcat Servers supports single sign-on (SSO) based on SAML. When users are authenticated at one site that participates in a single sign-on (SSO) configuration, they are automatically authenticated at other sites in the SSO configuration and do not need to log in separately.

The SAML standard defines a framework for exchanging security information within the federation of trusted servers.

The following steps describe a typical scenario that shows how SAML SSO works.

1. A Web user attempts to access a target resource at a site that is configured to accept authentications through SAML assertions. When configuring SAML 2.0 this site is called the Service Provider.
2. The Service Provider determines that the user's credentials need to be authenticated by a central site that can generate a SAML assertion for that user. The Service Provider redirects the authentication request to that central site. In SAML 2.0, the site that generates the SAML assertion is the Identity Provider. In both SAML versions, this site is sometimes called a SAML Authority.
3. The user logs in to the Identity Provider site, via a login web application hosted by that site. The Identity Provider authenticates the user, and generates a SAML assertion.
4. Information about the SAML assertion provided by the Identity Provider and associated with the user and the desired target is conveyed from the Identity Provider site to the Service Provider site by the protocol exchange. Through a sequence of HTTP exchanges, the user browser is transferred to an Assertion Consumer Service (ACS) at the Service Provider site. The WebLogic Server SAML Identity Assertion provider makes up a portion of the ACS.
5. The Identity Assertion provider maps the identity contained in the assertion to a Subject in the local security realm. The access policies on the requested target are evaluated to determine whether the user is authorized for that target. If access is authorized, the user authenticated by the Identity Provider site is accepted as an authenticated user by the Service Provider site, thereby achieving Web-based SSO.

2.5.2.1 Identity Provider Initiated Single Sign-On

In SSO infrastructure, the web user is authenticated by a common login application (NSW Login) deployed on the Identity Provider. Then, he/she is able to access the NSW web applications hosted by the Service Provider(s).

WebLogic and Tomcat Servers support this scenario in which a web single sign-on session is initiated by an Identity Provider. In this scenario, a user is authenticated by an Identity Provider and issues a request on a resource that is hosted by a Service Provider. The Identity Provider initiates the SSO session by sending an unsolicited authentication response to the Service Provider.

When the Service Provider receives the authentication response, the Service Provider extracts the identity of the user from the assertion, maps that identity to a local subject, and performs an authorization check on the requested resource. If the authorization check succeeds, access is granted.

Figure 2-2 shows – as an example - the flow of execution in a typical Identity Provider (WebLogic) initiated SSO session.

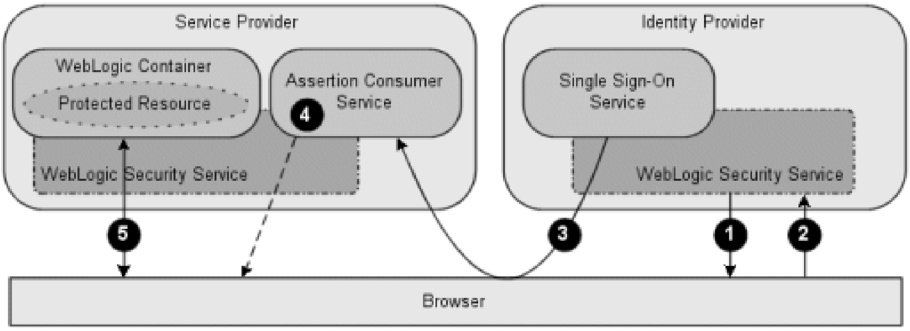


Figure 2-2 Identity Provider Initiated Single Sign-On.

The following steps describe the flow of execution:

1. The user is presented with a login web application hosted by an Identity Provider that authenticates the user. The Identity Provider challenges the user for his or her credentials.
2. The user provides his or her username and password to the Identity Provider, which completes the authentication process. The user issues a request on a resource that is hosted by a Service Provider.
3. The Single Sign-On Service hosted by the Identity Provider sends an unsolicited authentication response to the Service Provider to the Service Provider's Assertion Consumer Service (ACS).
4. The ACS validates the assertion, extracts the identity information, and maps that identity to a subject in the local security realm. The ACS sends an HTTP redirect message to the browser, passing a cookie containing a session ID and enabling the browser to access the requested resource.
5. The WebLogic Security Service performs an authorization check to determine whether the browser may access the requested resource. If the authorization check succeeds, access to the resource is granted.

2.6 Application Server

The WebLogic Server 11g is used to host NSW system, which provides the following functionality

- clustering feature provides increased scalability, availability and reliability
- WebLogic Server is compliant with Java Secure Socket Extension (JSSE). JSSE is a set of packages that support and implement the SSL and TLS v1 protocol.

  WebLogic Server provides Secure Sockets Layer (SSL) support for encrypting data transmitted across WebLogic Server clients, as well as other servers.

WebLogic Server supports the RSA cipher suites listed in COTS related documentation.

The current implementation of NSW uses Java platform.

Components used:

- JDK (1.7)
- Apache Tomcat 7.x

2.7 Database

Oracle RDBMS Server 11g shall be used for NSW data storage; Real Application Clusters (RAC) technology provides fault tolerance, security, load balancing, and scalability.

Alternatively PostgreSQL 9.x may be used.

2.8 Non-functional requirements

The non-functional requirements are addressed separately in terms of the architectural solution offered:

- Portability: The technical architecture solution is based on standard Java EE technologies. Any application server specific extensions/frameworks should be avoided where possible. Non portable parts of the NSW System, if applicable, should be isolated and documented.
- Scalability: The design of the system and selection of technologies support a scalable solution.

  Additionally, the NSW System includes software frameworks/products that are known to be scalable.
- Reusability: A design based on components lends support for reusability.
- Modularity: The NSW System is delivered as software components.
- Maintainability: The components are loosely coupled therefore they should require less maintenance overhead.
- Availability: The technical solution allows for the NSW System to be deployed onto more than one application server to meet availability demands.
- Performance: The design of the NSW System and selection of software products/frameworks has been undertaken with performance in mind to ensure the NSW services shall
  - Accept up to 1000 ship data providers accessing the web interfaces.

- Receive up to 6000-10000 clearance requests (including those reporting the cargo information) per day (submitted via system interface or via the web interface).
- Transmit up to 3000 revamped PortPlus notifications to SSN central system per day.
- Submit up to 3000 ShipCall requests to SSN central system per day.
- Complete the execution of actions initiated by a user using the web interface up to 3 seconds.

- Security: The infrastructure (router, reverse proxy, application server) hosts the NSW components shall provide security techniques for secure communication using TLS protocol 1.0 or later.

  The integrity of NSW communication shall be protected applying SSL encryption method with 128 bit or more symmetric key strength.

  OWASP Enterprise Security API (ESAPI) Project shall be used on the implementation of NSW web applications. The targeted level for the NSW is OWASP Level 2.

3 Overall System Architecture

3.1 Business Processes

This section describes the main business processes identified during the analysis of business requirements.

The methodology used for gathering all business processes identified on the ―Business Process Modelling Notation, also called BPMN.

The primary goal of the BPMN effort is to provide a notation that is readily understandable by all business users, from the business analysts that create the initial drafts of the processes, to the technical developers responsible for implementing the technology that will perform those processes, and finally, to the business people who will manage and monitor those processes.

Thus, BPMN creates a standardized bridge for the gap between the business process design and process implementation.

BPMN defines a Business Process Diagram (BPD), which is based on a flowcharting technique tailored for creating graphical models of business process operations.

A Business Process Model, then, is a network of graphical objects, which are activities (i.e., work) and the flow controls that define their order of performance.

Applicable business rules for data validation and processing are listed in Annex A: Business Rules.

3.1.1 Definitions

Statuses and Error Codes:

The following table lists the definition and permitted values for the Ship Call Status, the Request Status and the Request Error Codes.

No	Element	Definition	Permitted Values
1	Ship Call Type	Defines whether the Ship Call concerns an arrival in port or a departure from a port. Ship Call Type is defined by the Ship Data Provider.	➢ Arrival ➢ Departure
2	Ship Call Status	Defines the status of a Ship Call registered in the NSW and depends on the reported pre-arrival, arrival, departure or cancelation notification(s).	➢ Expected: In case of an Arrival Ship Call: no ATA is reported. In case of a Departure Ship Call: no ATD is reported. ➢ Arrived: the ATA is reported. This status is applicable only to Arrival Ship Calls. ➢ Departed: the ATD is reported. This status is applicable only to Departure

			Ship Calls. ➢ Closed: the Ship Call is considered closed and permits no further processing. ➢ Cancelled: a cancelation request was received. The Ship Call is cancelled. ➢ Draft (only via Web): The ship call is temporarily stored in the database for further processing. The request is NOT being forwarded to the authorities for clearance. Only after submitting the notification for clearance the request will be forwarded to the authorities and the Request status will become "Pending".
3	Request Status	In the CRG, it provides the overall decision (from all relevant authorities regarding a ship call. See business rule 33 and 42). In AIE it defines the status of the decision from each relevant authority regarding a ship call. NOTE: A draft ship call has no status. Once it is submitted for clearance then its request status will be "Pending". See also business rules 34, 35 and 36 in Annex A.	➢ Pending: The request has been forwarded to the authority(ies) and is pending decision by the authority(ies). ➢ Accepted: The ship call is accepted by the authority(ies). No further acknowledgement will be received. ➢ NotAccepted: The ship call is not accepted by the authority(ies).. The comment field will describe the reason.
5	Decision	Defines the decision taken by an authority as regards an individual data group	➢ Pending ➢ Accepted ➢ NotAccepted
4	Request Error Codes	Defines the error codes relevant to the processing of a clearance request.	➢ 0: Request was accepted and will be processed ➢ 1: SW does not accept multiple request updates. This request will be ignored and the original request will continue to be processed. ➢ 2: Too many copy-to entries. ➢ 3: The request did not contain enough information to continue processing. The request will be ignored.

			➢ 4: Business rule exception. ➢ 5: User does not have to necessary authorisation to provide such request. This may be because the user is unknown, does not have the right to send requests, does not have the right to send request for this port of call, or the request contains data elements that the user does not have the right to include in the request.

Profiles:

Access rights to the information and functionalities of the NSW are restricted based on the user profiles. A single user account is assigned a user profile. Three user profiles are considered: authority, ship data provider and national administrator. Each profile is assigned a list of tasks. The profile defines the maximum set of tasks a user can perform.

Tasks:

The task is defined as a function to be performed on a given group of data elements (entity). A user that will be assigned a task will be able to perform the indicated – by the task – action on the group of data elements. Functions are pre-defined based on the action:

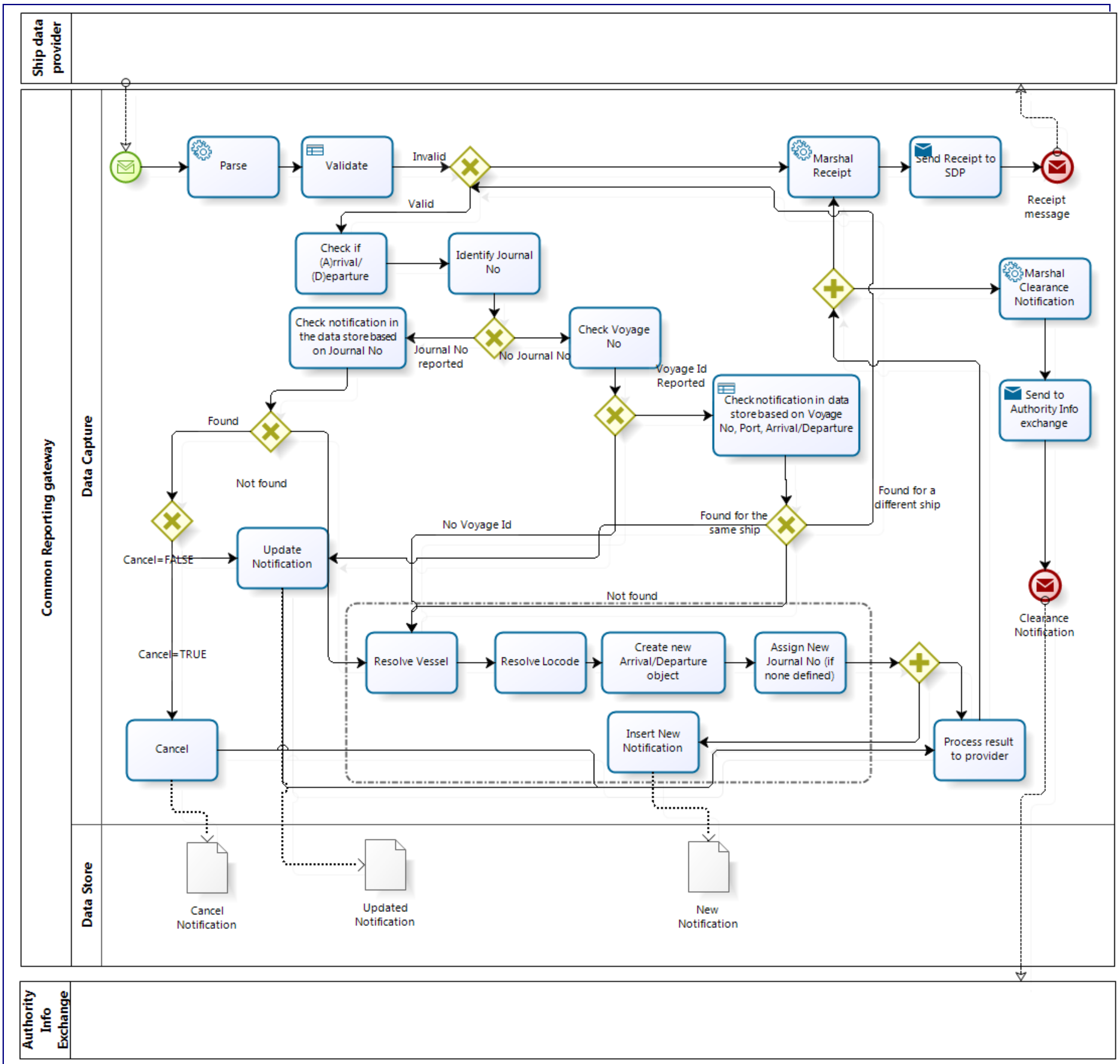
- PROVIDE
- CLEARANCE
- CONSULT
- MANAGE

For example, the task "PORT_CALL_PROVIDE" permits the user (i.e. ship data provider) to send notification information reporting Port call group data elements.

Annex B: Profiles and Tasks provides the lists of default profiles and tasks.

3.1.2 Data capture processes

Process Clearance Notification via XML	
Description:	The following diagram depicts the process of clearance notification received via the XML/SOAP interface.

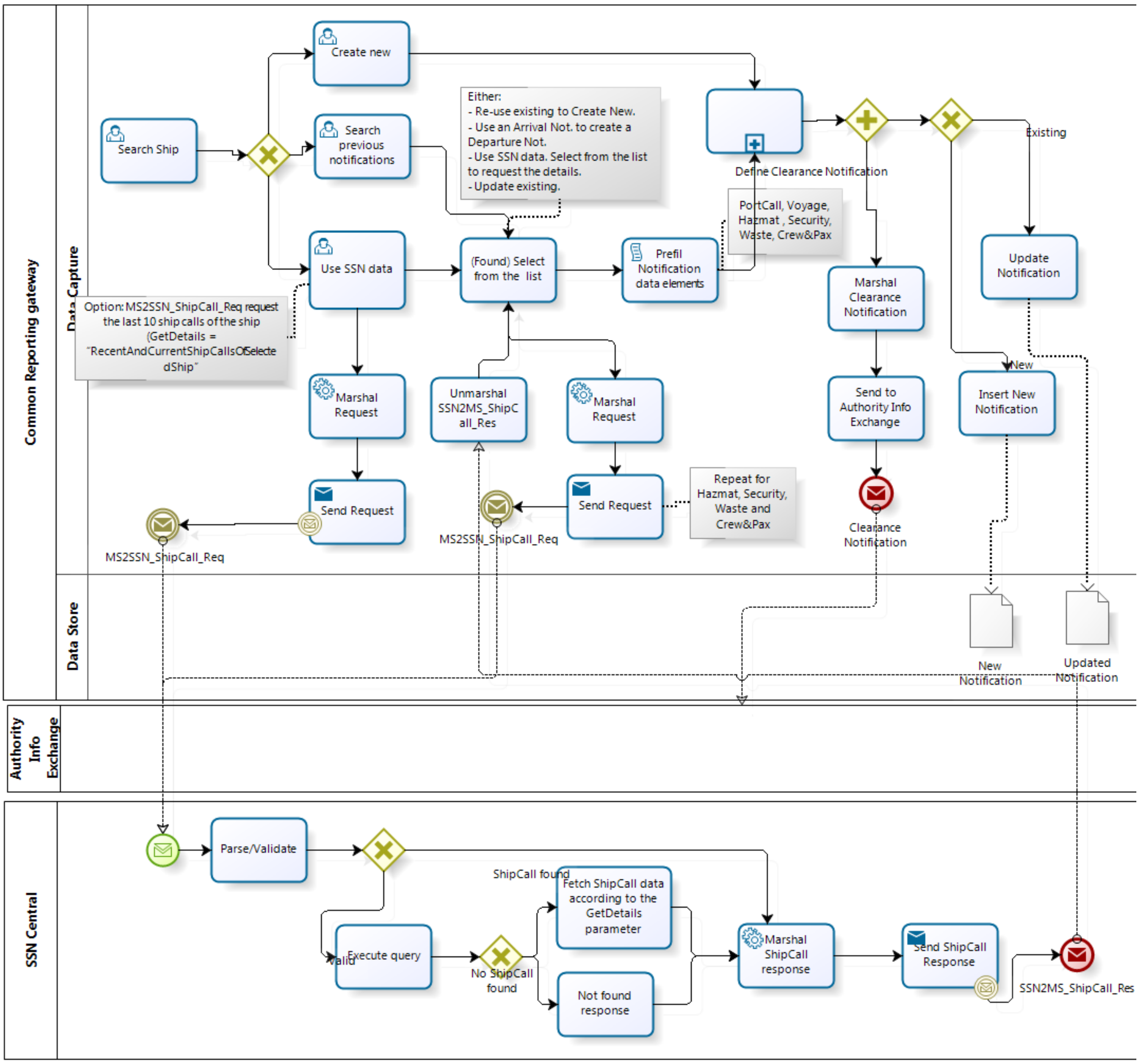


Step 1:	The process starts upon receipt of a clearance notification via the XML interface.
Step 2:	The Common Reporting Gateway shall provide a callback service to fulfil the receipt of clearance notification data.
Step 4:	The Common Reporting Gateway shall check/verify the accepted data / information. If there is a validation/verification error the process shall end.
Step 5:	The processing of information starts with the identification of the request being for an arrival to the port or departure from the port.
Step 6:	Check if Journal number is reported: - If yes then continue to step 7

	• If not then continue to step 8
Step 7:	This step is conditional to the result of step 6. Search the data store for a ship call that match the reported Journal number: • If found and the notification reports a cancelation then CANCEL the request. Update the status of the ship call in the data store to CANCEL. • If found and not CANCEL then go to step 9 • If not found then go to step 10
Step 8:	This step is conditional to the result of step 6. • If no Voyage number is reported then go to step 10 • If Voyage number is reported then search the data store for a ship call that matches the reported Voyage number, port of call and arrival/departure: o If found for the same ship then go to step 9 o If found for a different ship then the notification shall be rejected; go to step 13 o If not found then go to step 10
Step 9:	Update ship call in the data store with the new data / information reported. Update only the groups of data elements reported. Replace previous values with the latest reported in the notification.
Step 10:	This step of the processing includes the following (the execution of the next sub-steps shall be sequential due to their nature) i. Resolve the ship reported (identify and match the ship in the data store).If the ship is not defined in the data store and the ship IMO number is reported and valid while the rest of the identification elements reported are also valid then create a new record in the ships reference registry in the data store. ii. Resolve the Port of call reported (identify and match the location in the data store). If the Port of call is not defined in the data store and the is valid then create a new record in the locations reference registry in the data store. iii. Create a new ship call object with the data reported; iv. Generate and assign a new Journal number.
Step 11:	The Common Reporting Gateway shall insert/store the information to the data store.
Step 12:	The Common Reporting Gateway shall create or augment the descriptive information – from the consolidated data in the data store– and make it available to the Authorities.
Step 13:	At the end of the process, the Common Reporting Gateway shall return a receipt message to the ship data provider callback service.

Process Clearance Notification via Web

Description:	The following diagram depicts the process of clearance notification received via the Web interface.

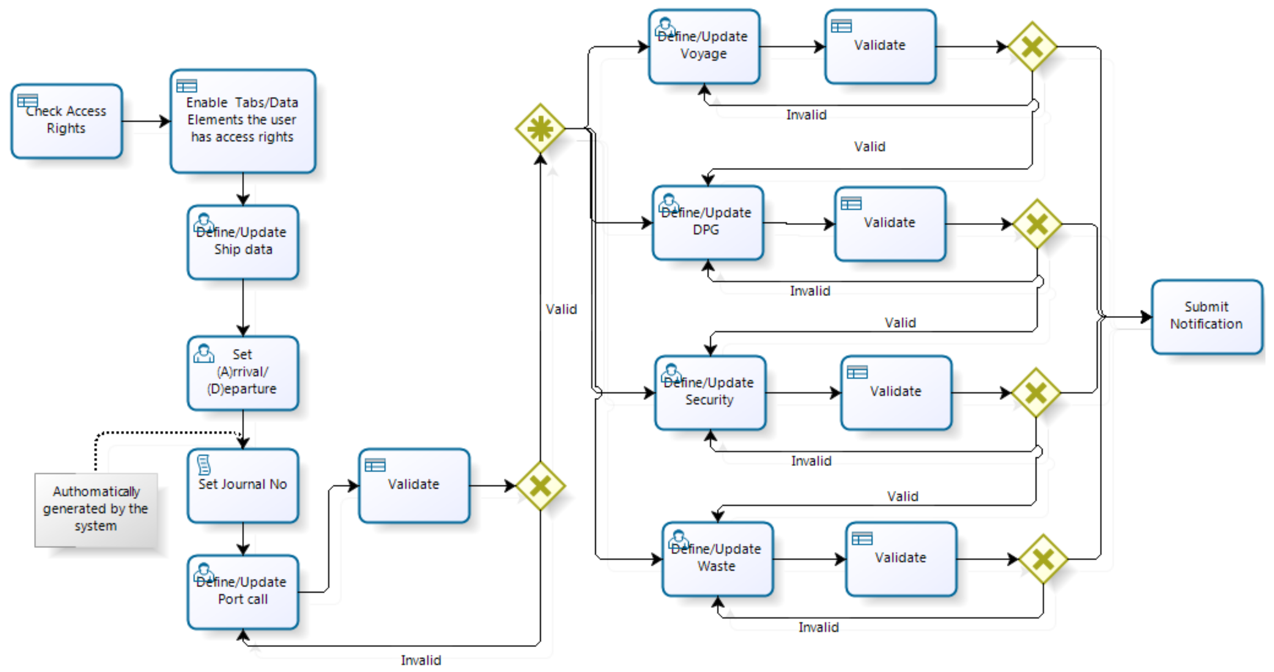

Common Reporting gateway
Data Capture
Data Store
Authority Info Exchange
SSN Central
Search Ship
Create new
Search previous notifications
Use SSN data
Either:
- Re-use existing to Create New.
- Use an Arrival Not. to create a Departure Not.
- Use SSN data. Select from the list to request the details.
- Update existing.
(Found) Select from the list
Prefil Notification data elements
Define Clearance Notification
PortCall, Voyage, Hazmat , Security, Waste, Crew&Pax
Existing
Update Notification
New
Insert New Notification
Marshal Clearance Notification
Send to Authority Info Exchange
Clearance Notification
Option: MS2SSN_ShipCall_Req request the last 10 ship calls of the ship (GetDetails = "RecentAndCurrentShipCallsOfSelectedShip"
Marshal Request
Send Request
MS2SSN_ShipCall_Req
Unmarshal SSN2MS_ShipCall_Res
Marshal Request
Send Request
MS2SSN_ShipCall_Req
Repeat for Hazmat, Security, Waste and Crew&Pax
New Notification
Updated Notification
Parse/Validate
valid
Execute query
ShipCall found
No ShipCall found
Fetch ShipCall data according to the GetDetails parameter
Not found response
Marshal ShipCall response
Send ShipCall Response
SSN2MS_ShipCall_Res

Step 1:	The ship data provider via the web shall be able to send a clearance notification.
Step 2:	Start by searching the data store for the ship. Once found the system shall fetch from the data store (if previously reported) the ship calls.

Step 4:	The user selects to: • Create a new ship call. Go to step 7 • Select an existing ship call to either: o Use the information to create a new arrival ship call. Go to step 6 o Use an arrival ship call to create a new departure ship call. Go to step 6 o Update an existing ship call. Go to step 6 • Use SSN data. Go to step 5
Step 5:	The Common Reporting Gateway shall create a ShipCall_Req to get the recent and current ship call of the selected ship and submit to SSN Central. SSN Central shall process the request and provide the ship calls found that satisfy the criteria will respond with a ShipCall_Res message. The CRG displays the port calls from SSN along with the list of ship calls of the NSW. Calls from SSN will be visually differentiated from the calls from the NSW and will have a "Re-use" button only. The user selects a port call from SSN. The CRG sends four MS2SSN_ShipCall_Req messages to request the detailed information regarding dangerous and polluting goods, waste, security and Crew & Passengers (one request for each). Once the four answers (SSN2MS_ShipCall_Res message) are received, the CRG uses the information to populate the forms of an arrival. Continue to the next step.
Step 6:	In case of using information from previously reported ship call, prefill data in the new notification except from (per case): • Create new from an existing one: "ETA to port of call", "ETD from port of call", "ATA port of call", "ATD port of call" and "ETA to next port" data. • Create a new departure from arrival notification: "ETA to port of call", "ATA port of call" and "ETA to next port" data. • Re-use from SSN: Data elements to re-use from SSN are indicated in [R10].
Step 7:	Define the Clearance Request Notification (see next sub-process).
Step 8:	The Common Reporting Gateway shall check/verify the complete data / information. If there is a validation/verification error the process shall end.
Step 9:	Update ship call in the data store with the new data / information reported. Update only the groups of data elements reported. Replace previous values with the latest reported in the notification.
Step 10:	The Common Reporting Gateway shall store the information to the data store.

	• In case of a new notification then insert new. • In case of update an existing then update ship call in the data store with the new data / information reported. Update only the groups of data elements reported. Replace previous values with the latest reported in the notification.
Step 11:	The Common Reporting Gateway shall create or augment the descriptive information – from the consolidated data in the data store– and make it available to the Authorities.
Step 12:	At the end of the process, the Common Reporting Gateway shall display a receipt message to the data provider.

Sub-process:	Define Clearance Notification

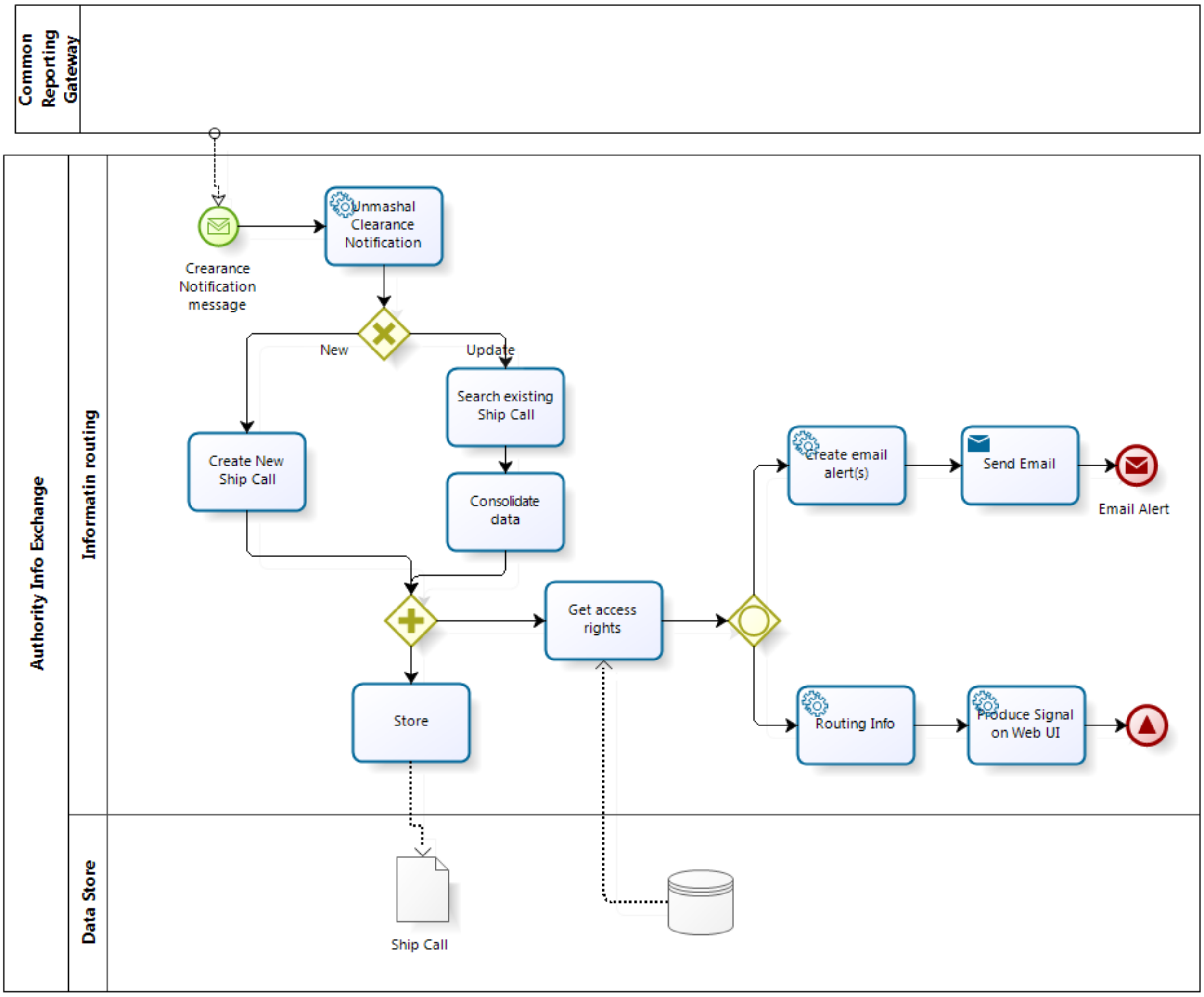


Step 7.1:	The Common Reporting Gateway checks the user access rights and enables only the tabs that correspond to the groups of data elements the user has the permissions to notify. A tab is enabled if the user has the access right for at least one of the groups in the tab. The elements of the group the user has no permission to notify are not editable.
Step 7.2:	The user defines/updates the ship tab data (groups “1. Ship identification” and “2. Ship particulars”).
Step 7.3:	The Common Reporting Gateway generates and assigns a new Journal number (if a new notification).
Step 7.4:	The user selects arrival or departure. The user defines the Port Call tab data (groups “3. Port call” mandatory,

	"4. Pre-arrival 72 hrs notification", "5. Arrival", "6. Departure", "7. Voyage"). Upon completion the system validates data and in case of error prompts the user to correct data.
Step 7.5:	This step includes the following (the execution of the next sub-steps can be done in any order provided that the groups of data are permitted to the user and the user is reporting them) i. Define/Update DPG tab data (groups "8. Dangerous and polluting goods", "9. Dangerous and polluting cargo items"); ii. Define/Update Security tab data (group 13. Security) iii. Define/Update Waste tab data (groups 11. Watse, 12. Waste disposal information); Similarly the user may define/update Ship Stores, Health, Cargo data etc. Upon completion of each sub-step the system validates data and in case of error prompts the user to correct data before moving on to the next sub-step.
Step 7.6:	The data object is submitted back to the main process.

3.1.3 Authority Information Exchange processes

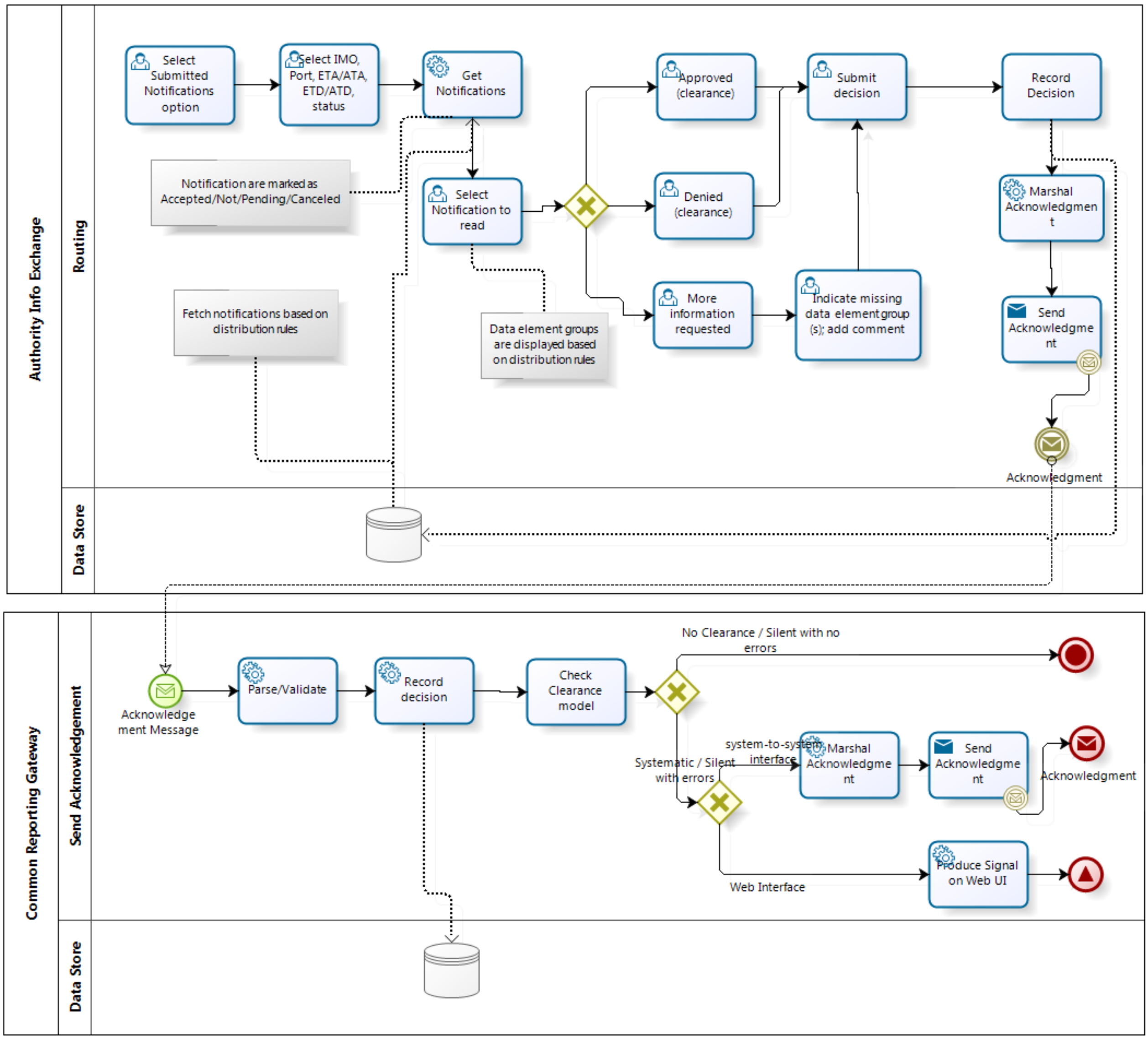
Process Clearance data routing	
Description:	The following diagram depicts the process of routing clearance notification data to the Authorities.



Step 1:	The process starts upon receipt of a consolidated Ship Call from the Common Reporting Gateway.
Step 2:	The information is stored in the AIE data store. In case of a new Ship Call insert a new Ship Call; in case of an update to an existing Ship Call then replace the Ship Call information.
Step 3:	The AIE checks the access rights of the Authorities to see which authority is relevant for the Ship Call (depending on the data included in the Ship Call).
Step 4:	Generate an email message and send it to the relevant Authorities to alert them of a new/updated request for clearance. Also produce a signal on the web interface to the relevant Authority user accounts to alert them of a new/updated request for clearance.

Process Acknowledgement

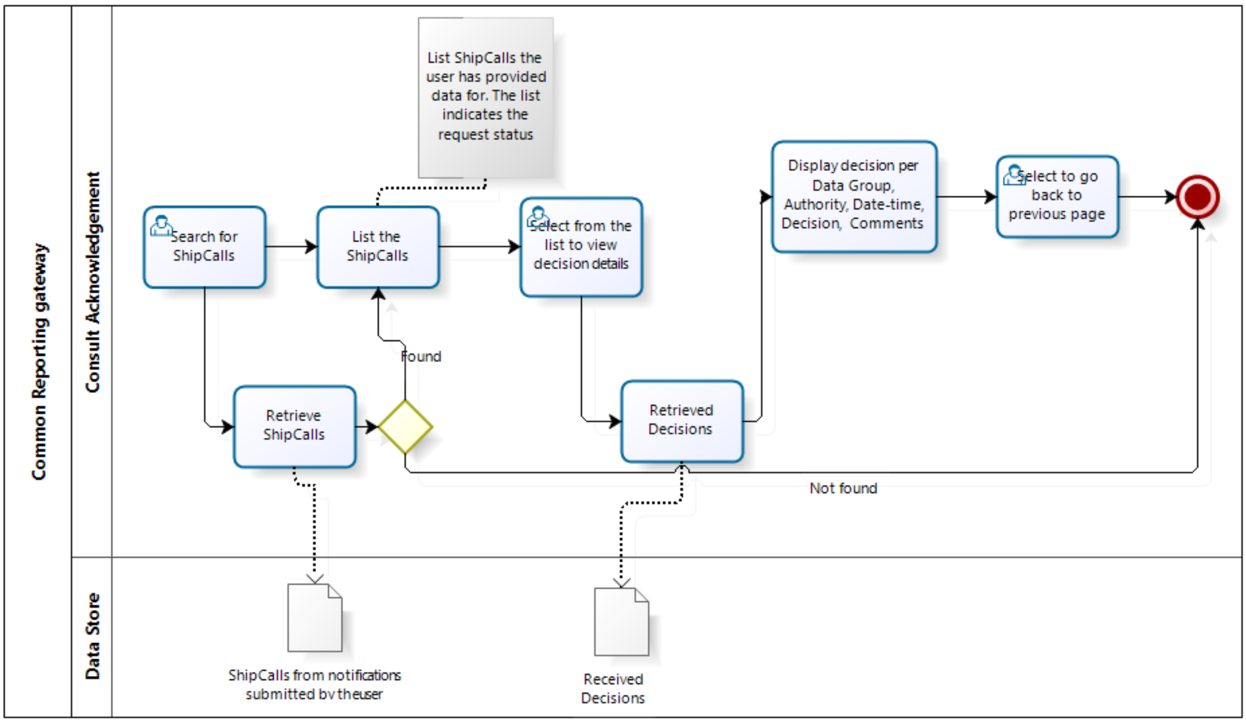
Description:	The following diagram depicts the process of acknowledging the clearance request.


Authority Info Exchange
Routing
Data Store
Select Submitted Notifications option
Select IMO, Port, ETA/ATA, ETD/ATD, status
Get Notifications
Notification are marked as Accepted/Not/Pending/Canceled
Select Notification to read
Fetch notifications based on distribution rules
Data element groups are displayed based on distribution rules
Approved (clearance)
Denied (clearance)
More information requested
Submit decision
Indicate missing data element group (s); add comment
Record Decision
Marshal Acknowledgment
Send Acknowledgment
Acknowledgment
Common Reporting Gateway
Send Acknowledgement
Data Store
Acknowledgement Message
Parse/Validate
Record decision
Check Clearance model
No Clearance / Silent with no errors
Systematic / Silent with errors
system-to-system interface
Marshal Acknowledgment
Send Acknowledgment
Acknowledgment
Web Interface
Produce Signal on Web UI

Step 1:	The authority via the web interface shall be able to select the Ship Call for acknowledgment. The authorities can only acknowledge Ship Calls for which they have the access rights to do so (this depends on the groups of data included in the Ship Call and the CLEARANCE tasks granted to the authority regarding these groups). It should be noted that an authority that is granted the CONSULT task for a group of data can only read the data of that group but cannot acknowledge that data group.
Step 2:	The user can search for notifications that are accepted or not-accepted or

	pending or cancelled. Start by searching the data store for Ship Calls pending acknowledgement by date and arrival/departure.
Step 3:	The NSW core fetches the list of Ship Calls that satisfy the criteria.
Step 4:	The authority selects from the list for further processing. Only the groups of data elements he/she has access rights for are accessible.
Step 5:	Record the decision and possible comments per group of data elements in the EPC_CLEARANCE_STATUS table: • Accepted: the clearance request is approved. • NotAccepted: the clearance request is denied. Submit decision.
Step 6:	The NSW core shall merge all acknowledgements from the authorities involved in the clearance process and record the decisions for the Ship Call per authority in the data store.
Step 7:	The NSW core shall create or augment the descriptive information – from the consolidated data in the data store– in an acknowledgement message.
Step 8:	At the end of the process, the NSW core shall return an acknowledgement message to the Common Reporting Gateway callback service. For information: The Common Reporting Gateway shall then record the decision in its data store and depending on the acknowledgement model configured at the NSW: • No clearance: end process. • Systematic clearance: The approval of clearance is consolidated before being communicated to the ship data provider. Based on the overall Request Status (as defined in section 3.1.1). Return an acknowledgement message to the ship data provider callback service (XML/SOAP) or produce a signal via the Web. • Silent clearance: in case of denial decision or request for additional information decision, each time such decision is recorded by an authority, return an acknowledgement message to the ship data provider callback service(XML/SOAP) or produce a signal via the Web.

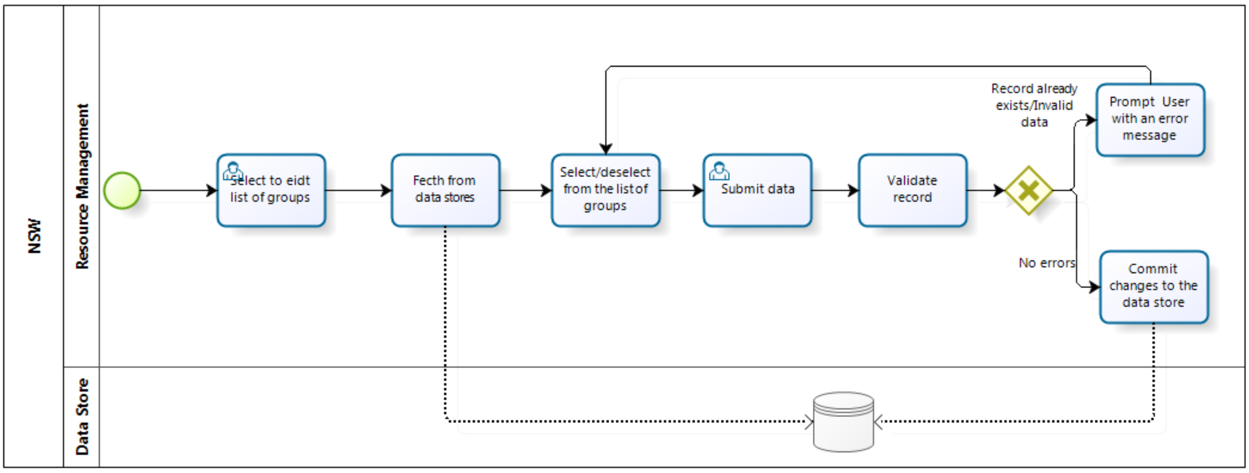
Process Consult Acknowledgement	
Description:	The following diagram depicts the process of consulting the acknowledgement of the clearance request.


Common Reporting gateway
Consult Acknowledgement
Data Store
List ShipCalls the user has provided data for. The list indicates the request status
Search for ShipCalls
List the ShipCalls
Select from the list to view decision details
Display decision per Data Group, Authority, Date-time, Decision, Comments
Select to go back to previous page
Retrieve ShipCalls
Found
Retrieved Decisions
Not found
ShipCalls from notifications submitted by the user
Received Decisions

Step 1:	The ship data provider via the web shall be able to consult the acknowledgement of a Ship Call previously submitted.
Step 2:	Start by searching the data store for the list of Ship Calls which the user has contributed to (he has submitted at least a notification regarding this Ship Call).
Step 3:	If ShipCalls found the system will fetch from the data store and display to the user. Proceed with step 4. If not found the list remains empty; end of process
Step 4:	The list displays the Ship Calls. From the list the user selects the desired Ship Call to view the decision(s).
Step 5:	The application retrieves the decision(s) from the data store and displays to the user.
Step 6:	The user may press the Back button to return to the previous page.

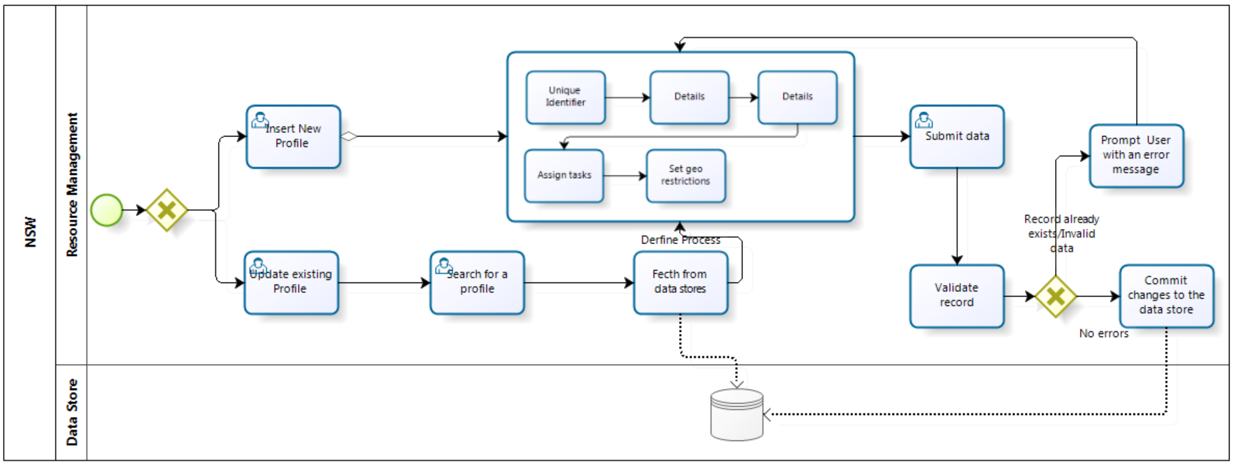
3.1.4 Configuration and Resource Management processes

Process Configure regulatory information	
Description:	Defines the steps executed by the national administrator to configure the groups of data elements of interest for the NSW The groups are defined in the data store. The attributes per group are predefined.


NSW
Resource Management
Data Store
Select to eidt list of groups
Fecth from data stores
Select/deselect from the list of groups
Submit data
Validate record
Record already exists/Invalid data
Prompt User with an error message
No errors
Commit changes to the data store

Step 1:	The National Administrator shall be able to edit the list of groups of interest to the data store.
Step 2:	Select the groups of interest. The groups Ship Identification and Port Call are mandatory (they are always of interest for the NSW).
Step 4:	NSW validates the set of groups to ensure: • Mandatory groups (Ship identification and Port Call) are selected; Based on the validation: • If mandatory groups are selected then proceed to the next step. • If not then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If validation was successful persist the configuration in the data store.

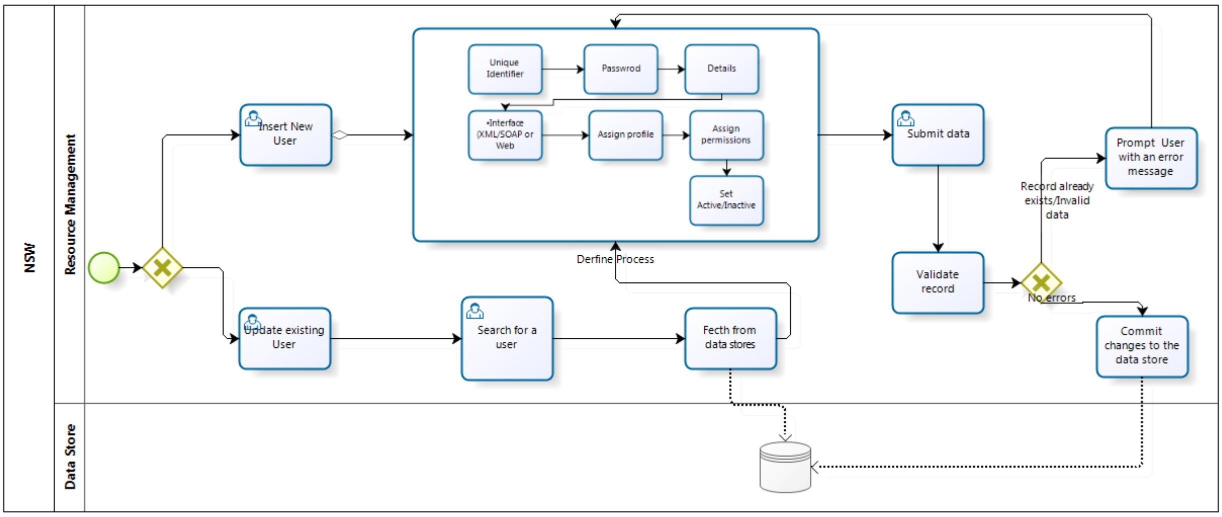
Process Configure access rights	
Description:	Defines the steps executed by the National Administrator to configure the access rights by associating the functions (tasks) on data groups to profiles. The default set of profiles have been defined in the data store. Tasks are predefined.



Step 1:	The National Administrator shall be able to insert new or update an existing profile.
Step 2:	Select to insert new profile. OR Select to update an existing profile; search the data store to fetch the matching record from the data store.
Step 3:	Complete the definition of: • The unique identifiers (name); • Other details (description); • Select to assign from the list of predefined tasks. Per task define the geographical restrictions at the level of Country/Area/Location. Once completed the data shall be submitted for validation and persistence.
Step 4:	NSW validates the record definition to ensure: • Uniqueness of identification; • Definition of mandatory attributes; • Correctness of data entered. Based on the validation: • If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then persist the record definition in the data store.

Process Manage User

Description: Defines the steps executed by the National Administrator to manage Users



Step 1: The National Administrator shall be able to insert new or update an existing user.

Step 2: Select to insert new user.

OR

Select to update an existing user; search the data to fetch the matching record from the data store.

Step 3: Complete the definition of:

- The unique identifiers (user id, first and last name);
- The password;
- Other details (location, contact details, shipping company);
- Interface (XML/SOAP or Web);
- Assign a profile (from the corresponding list);
- Assign permissions by selecting from the list of tasks of the assigned profile), adjust the geographical restrictions;
- Set active/inactive.

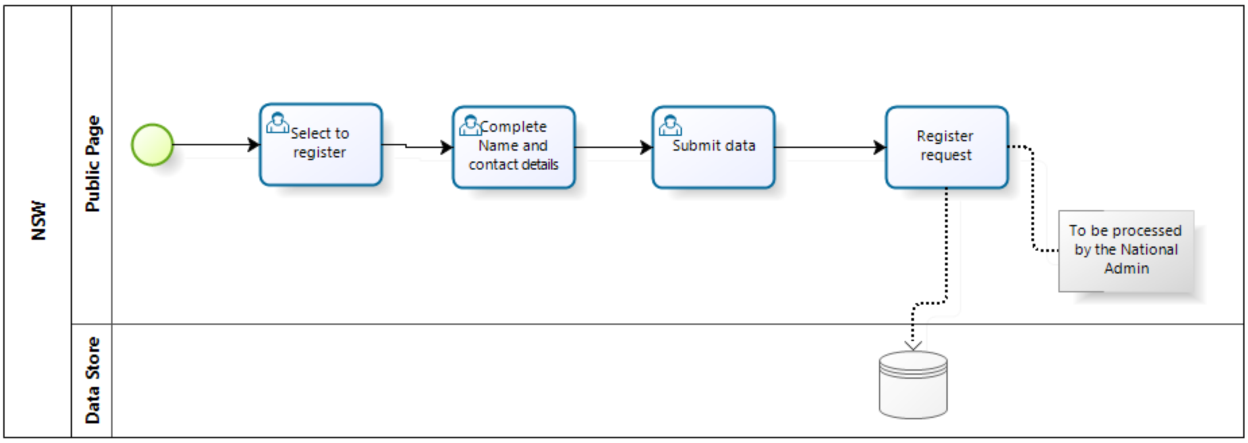
Once completed the data shall be submitted for validation and persistence.

Step 4: NSW validates the record definition to ensure:

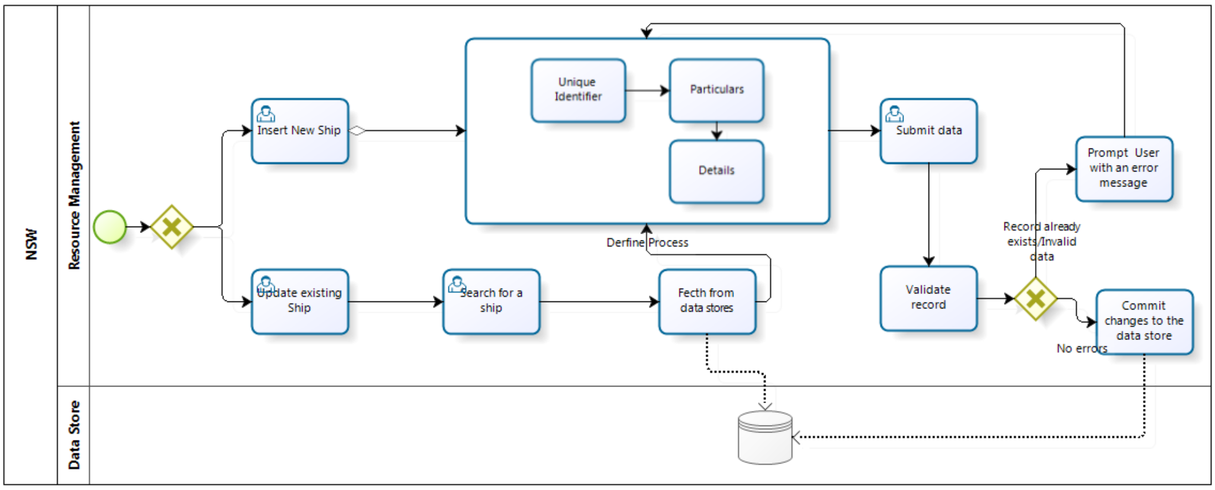
- Uniqueness of identification;
- Definition of mandatory attributes;
- Correctness of data entered.

Based on the validation:

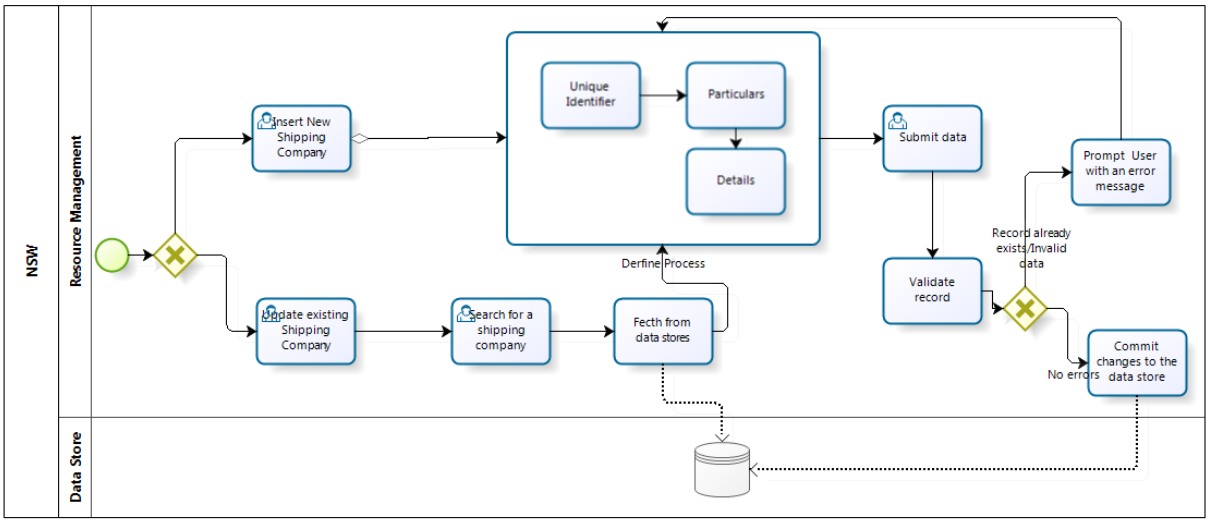
	• If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then persist the record definition in the data store.

Process Register to NSW	
Description:	Defines the steps executed by a User requesting access to the NSW. Registration is completed by the National Administrator via the manage user functions.
 NSW Public Page Data Store Select to register Complete Name and contact details Submit data Register request To be processed by the National Admin	
Step 1:	The User shall be able from a public URL to submit a request.
Step 2:	Select to register to NSW.
Step 3:	Complete the definition of: • Preferred unique identifiers (user id, first and last name); • The password; • Other details (location , contact details, shipping company, agencies); • Interface (XML/SOAP or Web); • Interest (in terms of Ship data provider/Authority); Once completed the data shall be submitted for validation and registration.
Step 4:	NSW validates the record definition to ensure: • Uniqueness of identification; • Definition of mandatory attributes; • Correctness of data entered. Based on the validation:

	• If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then register the request for processing by the National Administrator.

Process Manage Ship	
Description:	Defines the steps executed by the National Administrator to manage Ships
	
Step 1:	The National Administrator shall be able to insert new or update an existing ship.
Step 2:	Select to insert new ship. OR Select to update an existing ship; search the data store to fetch the matching record from the data store.
Step 3:	Complete the definition of: • The Ship identification elements (IMO (unique), MMSI, Name, CallSign, comments); • The Ship particulars elements (flag state, type, certificates, shipping company etc). Once completed the data shall be submitted for validation and persistence.
Step 4:	NSW validates the record definition to ensure: • Uniqueness of identification (IMO Number must be unique); • Definition of mandatory attributes: IMO Number;

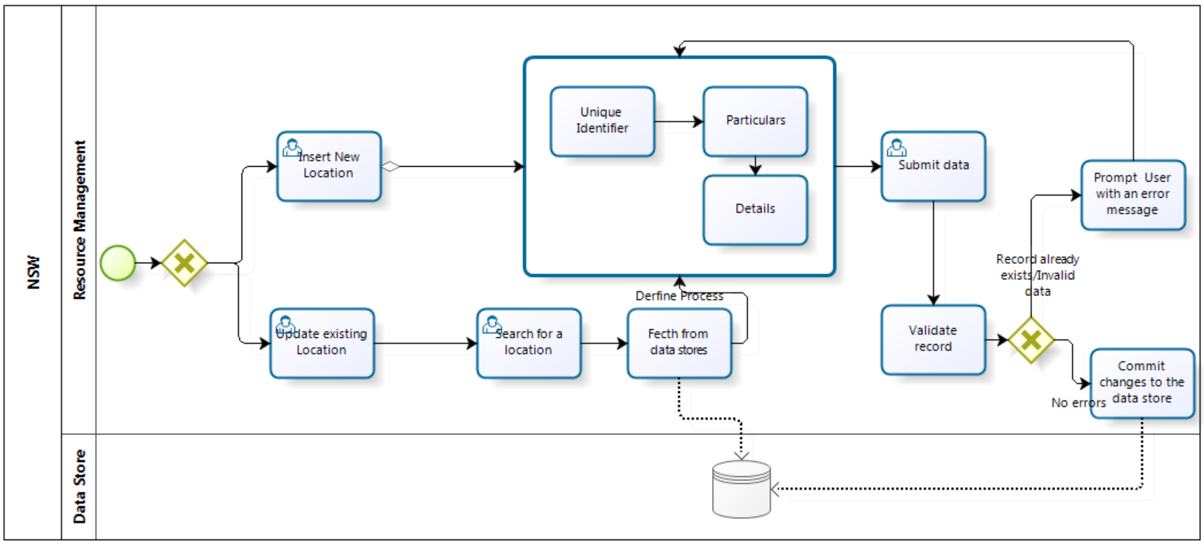
	• Correctness of data entered. Based on the validation: • If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then persist the record definition in the data store.

<table>
<tr><th colspan="2">Process Manage Shipping Company</th></tr>
<tr><td><b>Description:</b></td><td>Defines the steps executed by the National Administrator to manage shipping companies.</td></tr>
<tr><td colspan="2">
NSW
Resource Management
Data Store
Insert New Shipping Company
Unique Identifier
Particulars
Details
Submit data
Prompt User with an error message
Record already exists/Invalid data
Validate record
Commit changes to the data store
No errors
Derfine Process
Update existing Shipping Company
Search for a shipping company
Fecth from data stores

</td></tr>
<tr><td><b>Step 1:</b></td><td>The National Administrator shall be able to insert new or update an existing shipping company.</td></tr>
<tr><td><b>Step 2:</b></td><td>Select to insert new shipping company.
OR
Select to update an existing shipping company to fetch the matching record from the data store.</td></tr>
<tr><td><b>Step 3:</b></td><td>Complete the definition of:
• The unique identifier (IMO company number);
• The name;
• The location;
• Other details (contact details).
Once completed the data shall be submitted for validation and persistence.</td></tr>
</table>

Step 4:	NSW validates the record definition to ensure: • Uniqueness of identification; • Definition of mandatory attributes: IMO company number, name; • Correctness of data entered. Based on the validation: • If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then persist the record definition in the data store.

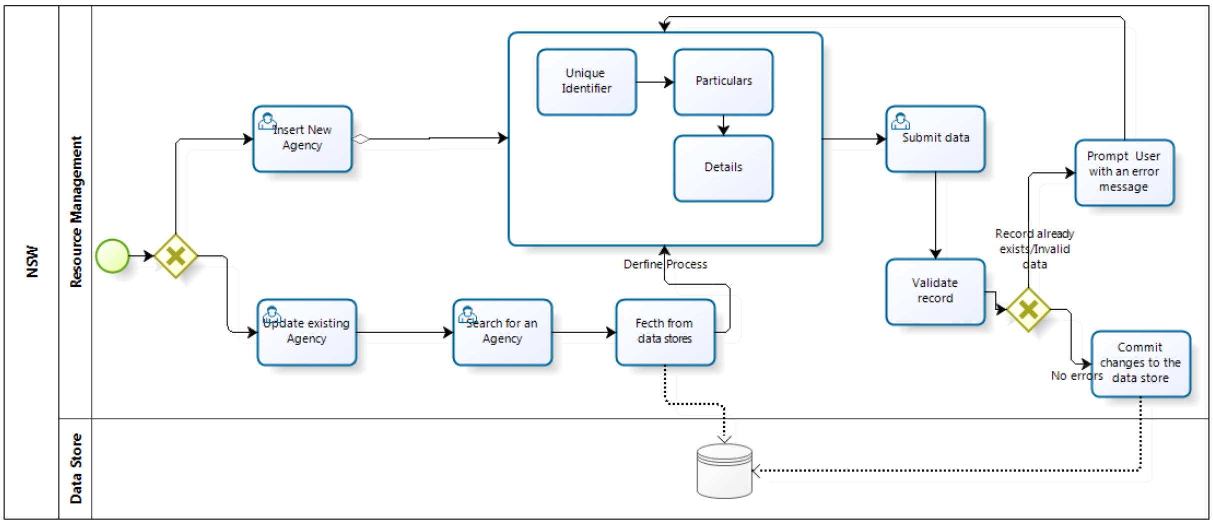
Process Manage Location	
Description:	Defines the steps executed by the National Administrator to manage Locations



Step 1:	The National Administrator shall be able to insert new or update an existing location.
Step 2:	Select to insert new Location OR Select to update an existing Location to fetch the matching record from the data store.
Step 3:	Complete the definition of: • The unique identifiers (LOCODE); • The particulars (country, name); • Other details (coordinates).

	Once completed the data shall be submitted for validation and persistence.
Step 4:	NSW validates the record definition to ensure: • Uniqueness of identification; • Definition of mandatory attributes; • Correctness of data entered. Based on the validation: • If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then persist the record definition in the data store.

Process Manage Agencies	
Description:	Defines the steps executed by the National Administrator to manage agencies.



Step 1:	The National Administrator shall be able to insert new or update an existing agent.
Step 2:	Select to insert new agency. OR Select to update an existing agency to fetch the matching record from the data store.
Step 3:	Complete the definition of:

	• The agency's name; • Other details (contact details). Once completed the data shall be submitted for validation and persistence. Name is trimmed, and multiple spaces are replaced by single space.
Step 4:	NSW validates the record definition to ensure: • Definition of mandatory attributes: name; • Uniqueness of name (search is not case sensitive and not diacritic sensitive); • Correctness of data entered. Based on the validation: • If valid record then proceed to the next step. • If invalid record then prompt the user with the errors and return to previous step.
Step 5:	Conditional to the validation result: If valid record then persist the record definition in the data store.

3.2 Functional Architecture

3.2.1 Use Case View

For the purposes of the use case definition the following actors and external systems are identified:

- Ship data provider (human via web or system via XML/SOAP) represents the external systems that submit regulatory information to NSW.
- Authorities (human): requests for clearance are being routed to authorities based on the distribution rules defined by the national administrator. Authorities may have one or several functions (e.g. Port authority, Hazmat authority, Security authority, Waste authority, Border control authority, Customs authority, Health authority, Port State Control authority).
- The national administrator (human) is in charge of the management of user accounts, use profiles and configuration of the NSW.
- SSN Central (system) will provide the revamp PortPlus message exchange services and ShipCall requests with NSW.

For identifying the functionality the typical UML use cases notation is used:

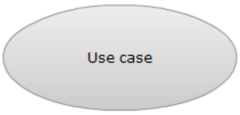
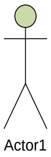
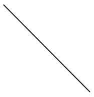
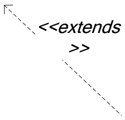
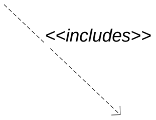
Symbol	Description
	**Use Case** - Represents a discrete unit of interaction between a user (human or machine) and the system. - Each Use Case has a description which describes the functionality that will be built in the proposed system. A Use Case may 'include' another Use Case's functionality or extend another Use Case with its own behaviour. - Use Cases are typically related to 'actors'.
	**Actor** - Human or machine entity that interacts with the system to perform meaningful work.
	**Association** - A relationship between two or more entities. Implies a connection of some type, for example one entity uses the services of another or one entity is connected to another over a network link.
	**Extends Relationship** - A relationship between two use cases in which one use case extends the behaviour of another.
	**Includes Relationship** - A relationship between two use cases in which one use case includes the behaviour.

Table 3-1: Use Cases Notation

The following diagram provides an overview of the NSW System Use Cases.

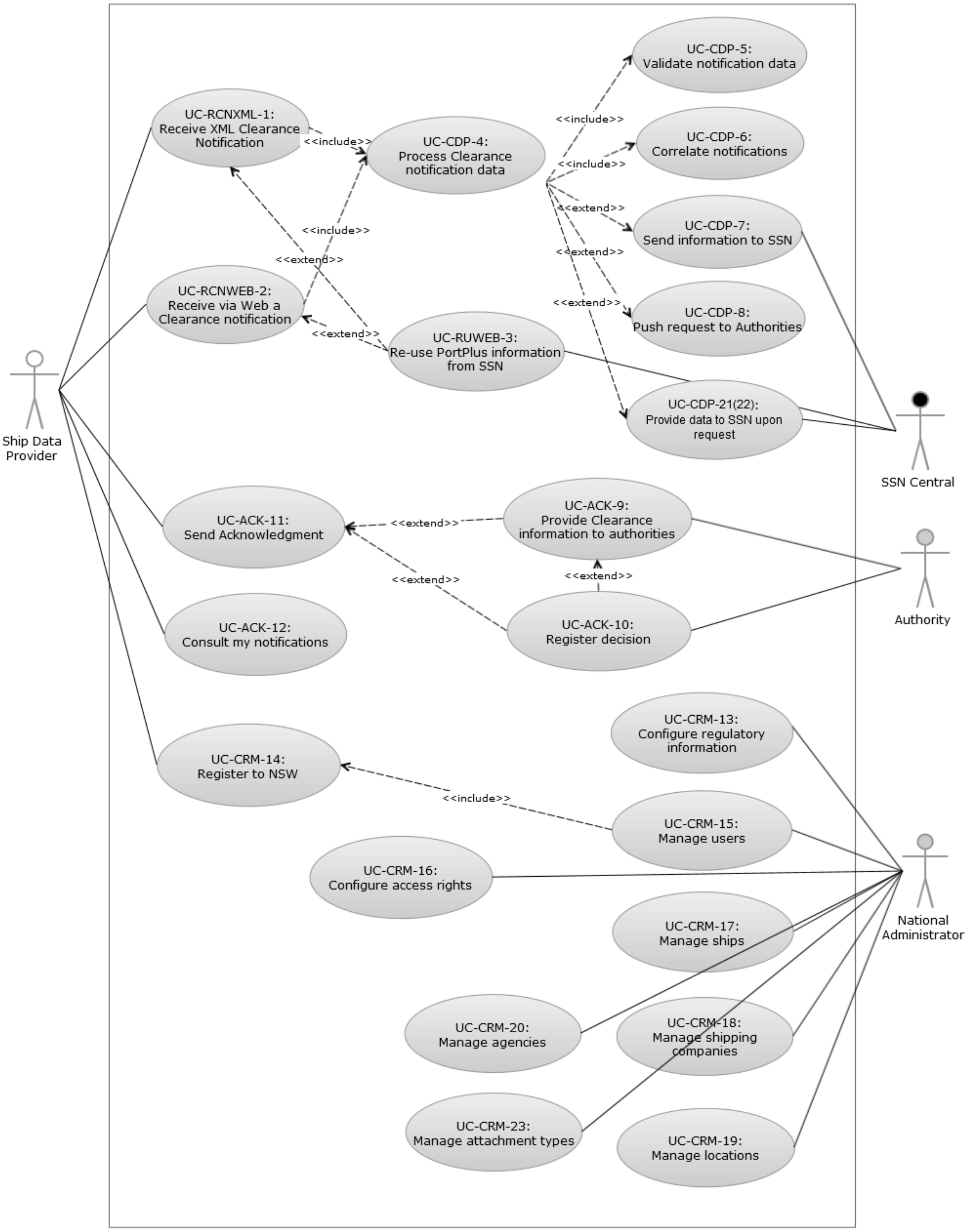


Figure 3-1 NSW Overall System Use Case diagram

3.2.1.1 Data Capture

This system package includes the services required in order for the NSW system to receive clearance notifications via the XML/SOAP and Web interfaces. More specifically, this system package consists of the following use-cases:

1. UC-RCNXML-1: Receive XML Clearance Notification
2. UC-RCNWEB-2: Receive via Web a Clearance notification
3. UC-RUWEB-3: Re-use PortPlus information from SSN

The use cases for the system-to-system interface and the web interface are distinct.

Use Case Req ID	**UC-RCNXML-1**
Use Case Name	**Receive XML Clearance Notification**
Purpose	This use case describes the system's functionality related to the submission via XML of a clearance notification prior to entry into ports or prior to departure from a port.
Subsystem	Common Reporting Gateway
Primary Actor(s)	Ship Data provider
Precondition(s)	The user must have a valid account and access rights to submit a clearance request. The ship and port call must be reported. More specifically the ship identification and port call groups must be reported in any new or complementary notification to be submitted.
Postcondition(s)	A new clearance notification is registered and identified by a unique "journal number".
Trigger(s)	Actor transmits an XML clearance notification message.
Use Case Description	Primary Workflow: [Valid Incoming Notification]
Step 1	The Common Reporting Gateway system is invoked to receive the incoming notification or from an external application.
Step 2	The Common Reporting Gateway system time stamps (in UTC) the incoming notification with the time of receipt.
Step 3	Validate the format and structure of the incoming notification against the predefined format (e.g. XML) and structure (e.g. corresponding XSD). The notification is found compliant with the predefined format and structure for the given interface.
Step 4	Log the receipt of a valid notification (notification identification, domain of interchange, originator of valid notification, date and time of receipt in UTC).
Step 5	The Common Reporting Gateway system propagates the received notification for data processing UC-CDP-4: "Process Clearance notification data" is executed.
Step 6	Log the notification (notification identification, domain of interchange,

	originator of valid notification, date and time of receipt in UTC).
Use Case Description	Alternative Scenario 1: [Invalid Incoming Notification]
Step 1.1	The notification cannot be parsed against the corresponding XSD format and structure. The Common Reporting Gateway system generates a rejection receipt and disseminates it to the notification sender.
Step 1.2	The Common Reporting Gateway system logs the parsing failure event (identifier of rejection notification, correlation identifier with erroneous notification, domain of interchange, originator of erroneous notification and receiver of rejection notification, date and time of submission in UTC).
Step 1.3 – Step 1.5	These steps are not applicable, since the notification format and structure validation has failed.
Step 1.6	Log the notification (notification identification, domain of interchange, originator of valid notification, date and time of receipt in UTC).
Input(s)	The primary clearance notification must report Arrival or Departure, the Ship Identification and Port call data groups that identify the ship and port call information. For the remaining data groups the data provider may report in the primary notification or complementary notification(s). – Ship identification (mandatory) – Ship particulars – Additional ship particulars – Port call (mandatory) – Additional port call information – Pre-arrival 72 hrs notification – Arrival – Departure – Voyage – Dangerous and polluting goods – Cargo Declaration – Consignment – Consignment – cargo details – Cargo Item – Cargo Item – cargo details – Cargo Item – DPG details – Ship's Stores – Waste – Waste disposal information – Waste delivery receipt – Security – Number of persons on board

	– Passengers – Crew – Crew's Effects – Health – Health - MDH Attachment – Bunkers remaining on-board – Civil Liability Certificate for Oil Pollution Damage – Civil Liability Certificate for Bunker Oil Pollution Damage – Ship defects
Output(s)	Receipt message with processed status code and in case of valid notification the assigned "journal number"; New clearance notification is recorded in the common reporting gateway or in case of update the existing clearance notification is updated.
Timer(s)	N/A
Business Process(es) Reference	Process Clearance Notification via XML
Associated Use Case(s)	Included Case: UC-CDP-4: Process clearance notification data
Special Requirements	A ship may be registered in the database; if not the reported ship is recorded in the ship database provided the ship identification is technically correct.

Use Case Req ID	**UC-RCNWEB-2**	
Use Case Name	**Receive via Web a Clearance notification**	
Purpose	This use case describes the system's functionality related to the submission via Web of a clearance notification for arrival or for departure.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	Ship Data provider Authority (assigned the relative task to update an existing Ship Call).	
Precondition(s)	The user must have a valid account and access rights to submit a clearance request.	
Postcondition(s)	The clearance notification is registered and identified by a unique "journal number".	
Trigger(s)	Actor submits a notification manually via the web.	
Use Case Description	Primary Workflow: [Valid Notification]	

Step 1	Search for a Ship by IMO Number, MMSI Number, Call Sign and/or Ship Name to fetch from the database the ship(s) that satisfy the criteria.
Step 2	Select a ship from the list to proceed.
Step 3	Search the database for ship calls of the selected ship based on: Port Of Call, Date (ETA/ATA for arrival notifications, ETD/ATD for departure notifications within 24H, 48H or 7 days), type (Arrival/Departure), CallStatus and Request Status. Optionally, send a request to SSN to retrieve ship calls of the selected ship. Such ship calls will be considered in addition to the ship calls from the database. The list will display per Ship Call all the columns mentioned above as search criteria and an additional column named Formalities (icons of the EPC notification tabs for which data is reported).
Step 4	Select one of the Ship Calls displayed. Then from the end of the page click on one of the buttons listed hereunder to proceed: • New notification. Send a new notification from the start. Select one of the 2 options: a) create a new arrival notification or b) create a new departure notification. The application will pre-fill the ship identification, ship particulars and CSO details (in the Security tab) from the database. • Re-use for new notification. Create a new notification from an existing ship call: use the data from an existing ship call to create a new notification. The application will pre-fill all data fields from the selected ship call except from the "ETA to port of call", "ETD from port of call", "ATA port of call", "ATD port of call" and "ETA to next port" data. In case the ShipCall is received from SSN Central the CRG will issue a ShipCall request to SSN Central for the Hazmat, Security, Waste and Crew & Passengers details. The CRG uses the information (if exist) to populate the forms of an arrival. Data elements to re-use from SSN are indicated in [R11]. • Update notification. This option is available only when the Ship Call status is "Expected", "Arrived" or "Departed". : select the ship call from the list. The application will pre-fill all data fields from the selected ship call. • Prepare departure notification. Send a new departure notification from arrival ship call: if the previous was an arrival ship call use to define the Departure notification. The application will pre-fill all data fields from the previous selected ship call except from the "ETA to port of call", "ATA port of call" and "ETA to next port" data. The SHIP_CALLS.PREVIOUS_SHIP_CALL_SID column for the new departure notification is assigned the value of the ship call ID from the arrival notification. • In case the departure notification reports an ATD from the port of call, update the relative arrival ship call by setting its status to "Closed."

	• Cancel call. • View decisions. Select to display the decisions recorded by the authorities so far. • View notification history. Select to display the list of notifications sent for the selected Ship Call. • Show ship on map. It will direct the user to the NSW GI interface and display the ship track on the map.
Step 5	Define clearance notification data. Data are grouped in tabs; each tab contains the groups of data elements as indicated hereunder: Ship tab – Ship identification (mandatory) – Ship particulars – Additional ship particulars Port tab – Port call (mandatory) – Additional port call information – Arrival – Departure – Number of persons on board Voyage tab – Voyage (except from Voyage Number which is not displayed) PSC tab – Pre-arrival 72 hrs notification DPG tab – Dangerous and polluting goods Cargo tab – Cargo Declaration – Consignment – Consignment - cargo details – Cargo item – Cargo item – Cargo details – Cargo item – DPG details Ship’s Stores – Ship's Stores Waste tab – Waste – Waste disposal information Waste receipt tab – Waste delivery receipt Security tab

- Security

Crew tab

- Crew

Passengers tab

- Passengers

Crew effects tab

- Crew's Effects

Health tab

- Health
- Health - MDH Attachment

Other tab

- Civil Liability Certificate for Oil Pollution Damage
- Civil Liability Certificate for Bunker Oil Pollution Damage
- Bunkers remaining on-board
- Ship defects

For each of the groups of data elements the user can attach none, one or more files (i.e. binary: picture, PDF, XLS, DOC). For each file he attaches, the user has to choose its type in a pre-defined list depending on the group (the list is configured by the NSW Administrator for each data group). The attachment will be associated with the specific data group.

The content of each tab is enabled or disabled according to:

- The type of notification: arrival or departure.
- The tasks granted to the ship data provider.

A tab that contains only groups of data elements that the user is not granted the corresponding task will not be accessible.

A tab that contains only data elements that are not included in the type (arrival/departure) of notification will not be accessible.

A tab that contains at least one group of data elements that the user is granted the corresponding task will be accessible.

However, only the elements of the group that the user has the task and only the elements of the commercially sensitive group which were submitted by a user associated with an Agency which is associated also to the user (according to BR#5) will be:

- editable (in case the user has the "PROVIDE_<entity>" task),
- readable but not editable (in case the user has the "CONSULT_<entity>" task),

As regards attached files, when the group is editable, then the user may download or remove files associated with the group or attach additional files. When the group is readable, the user may only download the attached files associated with the group.

The values of the elements for which the user has no task assigned, or for which the user has no access rights or are not included in the type (arrival/departure) of notification, will not be visible. The same will apply

	to files attached to the group. Please refer to Annex B: Profiles and Tasks for the list of tasks.
Step 6	The application validates each individual group of data elements and prompts the user with incorrect data entered. The user must correct to proceed.
Step 7	Submit clearance notification data.
Step 8	The Common Reporting Gateway system propagates the received notification for further data processing. UC-CDP-4: “Process Clearance notification data” is executed.
Step 9	Log the notification (notification identification, domain of interchange, originator of valid notification, date and time of receipt in UTC).
Use Case Description	Alternative Scenario 1: [Record a draft notification]
Step 1.1 – step 1.6	These steps are the same as in the primary workflow.
Step 1.7	Submit clearance notification data as “draft” for further processing.
Step 1.8	The only processing the common reporting gateway is proceeding to is the execution of the following use case: UC-CDP-5 Validate notification data
Step 1.9	Log the notification (notification identification, domain of interchange, originator of valid notification, date and time of receipt in UTC).
Input(s)	The clearance notification must report the Ship Identification and Port call data groups that identify the ship and port of arrival. For the remaining data groups the data provider may report in the primary notification or complementary notifications for the same ship and port call. – Ship identification (mandatory) – Ship particulars – Additional ship particulars – Port call (mandatory) – Additional port call information – Pre-arrival 72 hrs notification – Arrival – Departure – Voyage – Dangerous and polluting goods – Cargo Declaration – Consignment – Consignment – cargo details – Cargo item – Cargo item – cargo details – Cargo item – DPG details – Ship's Stores – Waste – Waste disposal information – Waste delivery receipt – Security – Number of persons on board – Passengers – Crew

	– Crew's Effects – Health – Health - MDH Attachment – Bunkers remaining on-board – Civil Liability Certificate for Oil Pollution Damage – Civil Liability Certificate for Bunker Oil Pollution Damage – Ship defects
Output(s)	User is prompted with a confirmation message with processed status code and in case of valid notification the assigned "journal number"; New clearance notification defines a new ship call in the common reporting gateway or in case of update the existing ship call is updated. If the clearance notification has been submitted as draft the new or updated ship call is defined with ship call status = DRAFT and common reporting gateway no longer accepts notifications for the same ship call.
Timer(s)	-
Business Process(es) Reference	Process Clearance Notification via Web
Associated Use Case(s)	– Included Case: UC-CDP-4: Process clearance notification data – Included Case: UC-CDP-5: Validate notification data.extendedCase: UC-RUWEB-3: Re-use PortPlus information from SSN
Special Requirements	The web pages shall be organised in a way that elements are grouped in tabs; each tabs includes one or more groups of data elements; the user will be able to define the values for elements for the groups he/she has the access rights for.

Use Case Req ID	**UC-RUWEB-3**	
Use Case Name	**Re-use PortPlus information from SSN**	
Purpose	The current use case describes the system's functionality related to the submission via Web of a new clearance notification when the Ship Data Provider requests for the previously reported PortPlus notification details from SSN Central.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	Ship Data provider	
Precondition(s)	The user has searched and selected a a ship for viewing the corresponding list of ship calls. User has clicked the "Use SSN data" button.	
Postcondition(s)	If exists in SSN Central the relative ShipCall data for the given ship are used to prefill elements of data groups Ship particulars, *Port Call, pre-Arrival, Voyage, Dangerous and polluting goods, Dangerous and polluting cargo items, waste, security and crew & passengers* of the Clearance Notification in the web page.	
Trigger(s)	Actor submits a request manually via the web.	

Use Case Description	Primary Workflow: [ShipCall data exist]
Step 1	The user selects the action "Use SSN Data" following the search for a ship and the display of the corresponding ship call list available in the CRG..
Step 2	The application creates a ShipCall request with RequiredResponseCriteria: – GetDetails: RecentAndCurrentShipCallsOfSelectedShip – (NumberOfCalls = 10) – TimePeriod: StartDateTime = Current Timestamp – ShipIdentification: the selected ship
Step 3	The CRG displays the port calls from SSN along with the list of ship calls of the NSW. Calls from SSN will be visually differentiated from the calls from the NSW and will have a "Re-use" button. The user selects a ShipCall and CRG will submit 4 request to SSN each one requesting details per case below: – GetDetails= SelectedShipCall and GetHazmat = HazmatDetails – GetDetails= SelectedShipCall and GetWaste = WasteDetails – GetDetails= SelectedShipCall and GetSecurity = SecurityDetails – GetDetails= SelectedShipCall and GetCrewAndPax = CrewAndPaxDetails (the system will produce one request for each).
Step 4	The CRG receives the responses from SSN Central. More specifically: – All the 4 responses are received containing details. – Some or all of the responses are received containing only summary. The rest contain details. The CRG uses the information to populate the forms of an arrival. If all the details are provided then all the corresponding fields are populated. If only summary is provided then only the corresponding fields are populated. The rules based on which the fields are populated are based on the indication of data elements to re-use from SSN are defined in [R10]. It shall be noted that the responses from SSN will contain the detailed information if they were provided to SSN and then to NSW or the summary information reported to SSN with the initial PortPlus notification.
Use Case Description	Alternative Scenario 1: [No ShipCall data exist]
Step 1.1	The user selects the action "Use SSN Data" following the search for a ship and the display of the corresponding ship call list available in the CRG
Step 1.2	The application creates a ShipCall request with RequiredResponseCriteria: – GetDetails = RecentAndCurrentShipCallsOfSelectedShip – (NumberOfCalls = 10) – TimePeriod (StartDateTime) = Current Timestamp – ShipIdentification = the selected ship
Step 1.3	The application receives a response from SSN Central with

	StatusCode="NotFound". The user is prompted with the message "No data found".
Step 1.4	Not applicable.
Use Case Description	Alternative Scenario 2: [ShipCall request GetDetails = RecentAndCurrentShipCallsOfSelectedShipExpectedCallOfSelectedShip time out
Step 2.1	Execute step 1
Step 2.2	Execute step 2
Step 2.3	The application receives no valid response from SSN Central within the timeout period (i.e. 60 seconds). The user is prompted with the message "No data found".
Step 2.4	Not applicable.
Use Case Description	Alternative Scenario 3: [ShipCall request for details time out]
Step 1.1	Execute step 1
Step 1.2	Execute step 2
Step 1.3	Execute step 3
Step 1.4	The CRG receives none or some of the responses to the 4 requests for details. More specifically: – None of the 4 responses are received before the expiration of the time out value (the default values defined in the SSN XMLRG V3). The CRG prompts the user with the message "No data found". – Only some of the responses are received within the time out value. The CRG uses the information to populate the forms of an arrival. If all the details are provided then all the corresponding fields are populated. If only summary is provided then only the corresponding fields are populated. The rules based on which the fields are populated are based on the indication of data elements to re-use from SSN are defined in [R10].
Input(s)	The ship particulars and current timestamp.
Output(s)	A ShipCall Response message is received from SSN Central containing the following data groups: – Ship identification – Ship particulars – Port call – Pre-Arrival 72hrs notification – Voyage – Dangerous and polluting goods – Consignment – Cargo item

	– Cargo item – DPG details – Waste – Security – Crew & Passengers
Timer(s)	-
Business Process(es) Reference	SSN Central identifies the Member State NSW as the ShipCall data requestor not the actual Ship Data Provider.
Associated Use Case(s)	-
Special Requirements	-

3.2.1.2 Clearance data processing

This system package includes the services required by the NSW for the incoming data processing (i.e. data reported in the clearance notification). More specifically, this system package consists of the following use-cases:

1. UC-CDP-4: Process clearance notification data
2. UC-CDP-5: Validate notification data
3. UC-CDP-6: Correlate notifications
4. UC-CDP-7: Send information to SSN
5. UC-CDP-21: Provide data to SSN upon request
6. UC-CDP-8: Push request to Authorities

Use Case Req ID	**UC-CDP-4**	
Use Case Name	**Process clearance notification data**	
Purpose	The purpose of this use case is to describe the actions that the Common Reporting Gateway shall perform for clearance notification data processing.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	N/A	
Precondition(s)	N/A	
Postcondition(s)	The received notification data are processed.	
Trigger(s)	Primary Workflow: A data event; that is an incoming clearance notification message (UC-RCNXML-1: Receive XML Clearance Notification) or a notification submitted by a Ship Data Provider via the web application (UC-RCNWEB-2: Receive via Web a Clearance notification). Alternative Scenario 1: A notification submitted by an authority via the web application (UC-	

	RCNWEB-2: Receive via Web a Clearance notification).
Use Case Description	Primary Workflow: [Start the pre-defined process]
Step 1	The Common Reporting Gateway invokes a pre-defined process and/or service for execution. The invocation of the selected pre-defined process and/or service is achieved by <<extending>> each of the corresponding use-cases with input parameters the Ship identity, the Port Of Call and the rest of the reported clearance notification data.

Step 2	The Common Reporting Gateway propagates (distributes) the received notification to the internal configured listeners for further data processing (including quality verification through business/semantic validations), registration (storage) and correlation to other data.
	The following use cases are executed in order:
	UC-CDP-5 Validate notification data;
	UC-CDP-6 Correlate notifications;
	UC-CDP-7 Send information to SSN;
	UC-CDP-8: Push request to Authorities.

Step 3	The Request Status is reset. All Acknowledgement messages associated to the Ship Call registered in the database are deleted.
Use Case Description	Alternative Scenario 1: [Start the pre-defined process, customized for notification updated by an authority]
Step 1	The Common Reporting Gateway invokes a pre-defined process and/or service for execution. The invocation of the selected pre-defined process and/or service is achieved by <<extending>> each of the corresponding use-cases with input parameters the Ship identity, the Port Of Call and the rest of the reported clearance notification data.
Step 2	The Common Reporting Gateway propagates (distributes) the received notification to the internal configured listeners for further data processing (including quality verification through business/semantic validations), registration (storage) and correlation to other data. The following use cases are executed in order: UC-CDP-5 Validate notification data; UC-CDP-6 Correlate notifications; UC-CDP-7 Send information to SSN.
Input(s)	– Ship Identity. – Port Of Call. – List of pre-defined processes and/or services.
Output(s)	N/A
Timer(s)	-
Business Process(es)	Process Clearance Notification via XML

Reference	Process Clearance Notification via Web
Associated Use Case(s)	– Included Case: UC-CDP-5 Validate notification data – Included Case: UC-CDP-6 Correlate notifications – Included Case: UC-CDP-7 Send information to SSN – Included Case: UC-CDP-8: Push request to Authorities
Special Requirements	N/A

Use Case Req ID	**UC-CDP-5**	
Use Case Name	**Validate notification data**	
Purpose	The purpose of this use case is to describe the actions that the Common Reporting Gateway shall perform in order to validate the clearance notification data received.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	N/A	
Stakeholder(s)	-	
Precondition(s)	N/A	
Postcondition(s)	Validation outcome indicating successful or failed validation results.	
Trigger(s)	System request via the extendedCase: UC-CDP-4: Process clearance notification data. More specifically, a data event has taken place, namely the receipt of a notification.	
Use Case Description	Primary Workflow: [Notification Validation Success: Valid Notification for existing ship and PortOfCall]	
Step 1	Validate the information reported by the ship data provider in the received notification: – Validate the user id against the registered users and ensure the user is granted with the access rights to send a clearance notification for the given port of call. – Validate the ship identification against the ship registry. The ship is identified/ resolved. If the ship MMSI Number, Call Sign, Ship Name and ship particulars reported are different from values for the ship identified by the IMO Number in the ships reference registry then the system will update the corresponding values. – Validate the Port Of Call and other Locations reported against the locations registry. The locations are identified/ resolved.	
Step 2	Validate the remaining information reported by the ship data provider in the received notification against the applicable business rules (ref: business rules defined in Annex A). Found to be correct.	
Step 3	The validation returns a “TRUE” value as an indication of the successful validation.	
Use Case Description	Alternative Scenario 1: [Notification Validation Success: Valid	

	Notification for new ship]
Step 1.1	Validate the information reported by the ship data provider in the received notification: – Validate the user id against the registered users and ensure the user is granted with the access rights to send a clearance notification for the given port. – Validate the ship identification against the ship registry. The ship is not identified. Check if ship particulars are technically correct (ref: business rules defined in Annex A). Ship reported is valid. If the ship is not defined in the data store and the ship IMO number is reported and valid while the rest of the identification elements reported are also valid then create a new record in the ships reference registry in the data store.
Step 1.2	Validate the remaining information reported by the ship data provider in the received notification against the applicable business rules (ref: business rules defined in Annex A). Found to be correct. All the mandatory elements for the type of ship call (Arrival/Departure) are provided. Moreover, if Departure elements are reported in an Arrival notification then the Departure elements are ignored (and vice versa).
Step 1.3	The validation returns a “TRUE” value as an indication of the successful validation.
Use Case Description	Alternative Scenario 2: [Notification Validation Failure: Unauthorised user]
Step 2.1	Validate the information reported by the ship data provider in the received notification: Validate the user id against the registered users and ensure the user is granted with the access rights to send a clearance notification for the given port of call. User id is not registered or is not granted the required access rights. In case of an update, verify that the user submitting the notification is not associated with the Agency of the user that sent the original notification. The user attempts to update one of the data groups subject to BR#5 and is not associated to a correct Agency.
Step 2.2	This step is not executed if during the previous step errors were identified.
Step 2.3	The validation returns the error code relevant to the processing of a clearance request (ref: Request Error Codes defined in section 3.1.1).
Use Case Description	Alternative Scenario 3: [Notification Validation Failure: Invalid data]
Step 3.1	Validate the information reported by the ship data provider in the received notification: Check if ship particulars are technically correct (ref: business rules defined in Annex A). Ship reported is not technically correct. OR

	Validate the Port Of Call and other Locations reported against the locations registry. At least one location is not identified. OR they are both correct in which case progress to next step.
Step 3.2	This step is not executed if during the previous step errors were identified. Validate the remaining information reported by the ship data provider in the received notification against the applicable business rules (ref: business rules defined in section 3.1). Incorrect data found
Step 3.3	The validation returns the error code relevant to the processing of a clearance request (ref: Request Error Codes defined in section 3.1.1).
Input(s)	Input(s) passed from the extended Case: UC-CDP-4: Process clearance notification data: An incoming notification
Output(s)	Validation outcome: – Indication of successful or unsuccessful validation; and – Validated notification, in case of successful validation; or – Request Error Codes defined in section 3.1.1, in case of failed validation.
Timer(s)	-
Business Process(es) Reference	Process Clearance Notification via XML Process Clearance Notification via Web
Associated Use Case(s)	-
Special Requirements	The ship data registry is populated. The Locations data registry is populated.

Use Case Req ID	**UC-CDP-6**	
Use Case Name	**Correlate notifications**	
Purpose	The purpose of this use case is to describe the actions that the Common Reporting Gateway shall perform in order to correlate a subsequent notification sent following the 1st notification for the same ship call.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	N/A	
Precondition(s)	N/A	
Postcondition(s)	Notifications related to a particular ship call are correlated and their data are merged. If no relation is identified a new ship call is defined or the notification is rejected.	
Trigger(s)	System request via the extended Case: UC-CDP-4: Process clearance notification data. More specifically, a data event has taken place, namely the receipt of a notification. Timer, scheduled once a day, triggers the process to identify departure	

	ship calls with ATD past the current timestamp minus 7 days.
Use Case Description	Primary Workflow: [Correlation Success: Journal Number is reported]
Step 1	Check that the Journal Number is registered in the NSW and is assigned to a previously reported ship call. The Journal Number is found.
Step 2	The correlation returns a "TRUE" value as an indication of the successful correlation.
Step 3	The registered ship call is updated with the data from the new notification reporting the same Journal Number. The value of each XML EPCMessage element reported in the new notification updates the value of the corresponding column for the ship call in the database. In case an XML EPCMessage element is not reported the value of the corresponding column remains unchanged.
Step 4	In case of a departure notification that reports an ATD from the port of call, check for: • the associated arrival ship call, or • if there is no associated arrival ship call, the relative arrival ship call based on the reported ship, port and closest ATA (or ETA in case no ATA is reported yet). If found then change its status to "Closed."
Use Case Description	Alternative Scenario 1: [Correlation Success: Voyage Number is reported; Journal Number is not reported]
Step 1.1	Check that the Voyage Number is registered in the NSW and is assigned to a registered ship call. The Voyage Number is found. Check the Ship, Port Of Call and indication for Arrival/Departure between the registered ship call and the new notification message. – The Ship, Port Of Call and indication for Arrival/Departure are the same.
Step 1.2a	The correlation returns a "TRUE" value as an indication of the successful correlation.
Step 1.3a	The registered ship call is updated with the data from the new notification reporting the same Voyage Number.
Step 1.4a	In case of a departure notification that reports an ATD from the port of call, check for: • the associated arrival ship call, or • If there is no associated arrival ship call, the relative arrival ship call based on the reported ship, port and closest ATA (or ETA in case no ATA is reported yet). If found then change its status to "Closed."
Use Case Description	Alternative Scenario 2: [Correlation Failed: New Ship Call; neither Journal nor Voyage numbers are reported or the Voyage number is reported for a different Port of Call or Arrival/Departure indicator]
Step 2.1	The notification reports neither Journal Number nor Voyage number.

	OR The Voyage number is reported. Check that the Voyage Number is registered in the NSW and is assigned to a registered ship call. The Voyage Number is found. Check the Ship, Port Of Call and indication for Arrival/Departure between the registered ship call and the new notification message. – The Ship is the same but the Port Of Call is not the same. The Ship and Port Of Call are the same but the indication for Arrival/Departure is not the same. OR The Voyage number is reported. Check that the Voyage Number is registered in the NSW and is assigned to a registered ship call. The Voyage Number is not found.
Step 2.2	The correlation returns a "FALSE" value as an indication of the failed correlation.
Step 2.3	A new Journal Number is generated based on a dedicated database sequence that generates unique numbers. The Journal_Number is the concatenation of the NSW Country ISO alpha-2 code and the sequence number. A new ship call is registered with the data from the new notification.
Step 2.4a	In case of a departure notification that reports an ATD from the port of call, check for: • the associated arrival ship call, or • If there is no associated arrival ship call, the relative arrival ship call based on the reported ship, port and closest ATA (or ETA in case no ATA is reported yet). If found then change its status to "Closed."
Use Case Description	Alternative Scenario 3: [Correlation Failed: Journal Number not defined; Voyage Number is defined but corresponds to a different ship]
Step 3.1	Check that the Voyage Number is registered in the NSW and is assigned to a registered ship call. The Voyage Number is found. Check the Ship. The combination of values does not match between the registered ship call and the new notification message.
Step 3.2	The correlation returns a "FALSE" value as an indication of the failed correlation.
Step 3.3	Notification shall be rejected.
Use Case Description	Alternative Scenario 4: [Correlation Failed: Journal number is reported but is not registered in NSW]
Step 4.1	The Journal Number reported is not registered in the NSW.
Step 4.2	The correlation returns a "FALSE" value as an indication of the failed correlation.
Step 4.3	Notification shall be rejected.

Use Case Description	Alternative Scenario 5: [Correlation Failed: Ship Call status is "Closed" or "Cancelled"]
Step 4.1	The recorded Ship Call status is assigned the values "Closed" or "Cancelled" which permits no further processing.
Step 4.2	The correlation returns a "FALSE" value as an indication of the failed correlation.
Step 4.3	Notification shall be rejected.
Use Case Description	Alternative Scenario 5: [Correlation Failed: Journal_Number is reported. A Clearance Notification updates an existing Ship Call and attempts to change the Ship Call Type, or the IMO number of the ship]
Step 4.1	The Ship Call Type is different OR The IMO number of the ship is different.
Step 4.2	The correlation returns a "FALSE" value as an indication of the failed correlation.
Step 4.3	Notification shall be rejected.
Use Case Description	Alternative Scenario 6: [A departure ship call with ATD past the current timestamp minus 7 days is identified.]
Step 6.1	Search for departure ship calls with ATD past the current timestamp minus 7 days. Ship call(s) found.
Step 6.2	Update its status to "Closed."
Input(s)	Input(s) passed from the extended Case: UC-CDP-4: Process clearance notification data: An incoming notification
Output(s)	Correlation outcome: – Indication of successful or unsuccessful correlation; and – Updated ship call, in case of successful correlation based on the reported Journal Number; or – Updated ship call, in case of successful correlation based on the reported Voyage Number (when no Journal Number is reported); or – New ship call, in case neither the Journal Number nor the Voyage Number are reported; or – New ship call, in case no journal number is reported and the Voyage number is reported for a different Port of Call or Arrival/Departure indicator; or – Error data, in case of failed correlation and Voyage Number uniqueness violation. – Error data in case of failed correlation and Journal Number uniqueness violation.
Timer(s)	-

Business Process(es) Reference	Process Clearance Notification via XML Process Clearance Notification via Web
Associated Use Case(s)	-
Special Requirements	N/A

Use Case Req ID	**UC-CDP-7**
Use Case Name	**Send PortPlus notification to SSN**
Purpose	The current use case describes the functionality related to the transmission of a PortPlus notification to SSN Central based on the clearance notifications received by the Common Reporting Gateway.
Subsystem	PortPlus management
Primary Actor(s)	N/A
Precondition(s)	A clearance notification for a ship with an identified IMO Number and/or MMSI Number is received by the ship data provider and is successfully validated and correlated with existing ship call by the Common Reporting Gateway.
Postcondition(s)	A V3 MS2SNN_PortPlus_Not message is successfully sent to SSN Central. SSN Central sends an SSN_Receipt with StatusCode="OK".
Trigger(s)	A data event has taken place; the CRG receives a new or updated clearance notification.
Input(s)	Registered ship call data (that contains the consolidated data from notifications received).
Output(s)	A V3 MS2SN_PortPlus_Not message is transmitted to SSN Central. The PortPlus notification must report the Ship Identification and Port call elements that identify the ship and port of call. – Ship identification (mandatory) – Ship particulars – Port call (mandatory) – Pre-arrival 72 hrs. notification – Arrival – Departure – Voyage – Dangerous and polluting goods information for arrival/departure from the port of call – Waste – Security – Crew and passengers information for arrival/departure from the port of call (conditional: if the value of the APPLICATION_PARAMETER for sending CrewAndPax info to SSN is set to "activate") SSN_Receipt message with processed status code "OK" received from SSN Central.
Timer(s)	-

Business Process(es) Reference	-
Associated Use Case(s)	-
Special Requirements	A PortPlus is created based on the latest elements reported in the clearance notification. SSN Central rules relative to new and updates PortPlus notifications must be respected to ensure the proper consolidation of voyage specific data for a ship. A ship must be identified by IMO/MMSI number. SSN Central identifies the Member State NSW as the data provider for the PortPlus notification (field "From") not the actual ship data provider. A new notification will cause a new PortPlus with UpdateStatus="N" to be submitted to SSN Central. The PortPlus notification is assigned an MSRefId value that is generated based on a dedicated database sequence that generates unique integers concatenated with the unique_id by which SSN Central identifies the NSW. Any complementary notification will cause a new PortPlus with UpdateStatus="U" to be submitted to SSN Central. The PortPlus notification is identified by the ShipCallId. To ensure uniqueness the ShipCallId is assigned the value of the Journal number assigned to the ship call. The following conditions apply: – In case of an arrival notification the ShipCallId takes the value of the Journal Number. – In case of a complementary arrival notification that cause a new PortPlus with UpdateStatus="U" the ShipCallId takes the again value of the Journal Number, which is equal to the value of the ShipCallId of the PortPlus notification with UpdateStatus="U". – In case of a departure notification the system checks the value of the SHIP_CALLS.PREVIOUS_SHIP_CALL_SID column. If not null then check the previous ship call to be arrival and get the Journal Number. The Journal number is then assigned to the ShipCallId of the PortPlus notification to report the departure of the ship from the port of call. If no previous ship call is identified (SHIP_CALLS.PREVIOUS_SHIP_CALL_SID is null indicating that no arrival notification has been received for this ship), then the system will assign the Journal Number of the departure notification to the ShipCallId of the PortPlus notification. If the value of the APPLICATION_PARAMETER for sending CrewAndPax info to SSN is set to "activate" then the PortPlus notification shall contain the CrewAndPax data for the arrival (element "Crew&PaxNotificationOnArrival") or departure from the port (element "Crew&PaxNotificationOnDeparture") respectively. If the value is set to "deactivate" then the PortPlus notification shall not contain any CrewAndPax data (e.g. no element "Crew&PaxNotificationOnArrival", no element "Crew&PaxNotificationOnDeparture").

Use Case Req ID	**UC-CDP-21**	
Use Case Name	**Provide data to SSN upon request**	
Purpose	Covers the functionality related to the systems' actions upon receiving a request for ship call details from SSN Central	
Subsystem	PortPlus management	
Primary Actor(s)	SSN Central	
Precondition(s)	A request for information has been received by the system.	
Postcondition(s)	The system has processed the request.	
Trigger(s)	A request for information has been sent to NSW in XML format	
Use Case Description	Primary Workflow (ShipCall is identified, NSW responds to the request)	
Step 1	The SSN Central has sent a valid request for information (SSN2MS_ShipCall_Req with From="SSN").	
Step 2	The System identifies the request parameters: ShipCallResp – GetHazmat (optional) – GetWaste (optional) – GetSecurity (optional) – GetCrewAndPax (optional) AdditionalSearchCriteria – ShipCallId (mandatory) – GetHazmatType (optional) – GetCrewAndPaxType (optional)	
Step 3	Searches the database for a relevant ship call (based on the ShipCallId which shall match the Journal Number of an existing ship call previously reported to SSN Central).SSN Central will only request for a ShipCallId previously notified by the NSW.	
Step 4	The ship call is identified. The system will search and fetch: - VesselIdentification, VoyageInformation from the arrival notification if the request is for Waste, Security, Hazmat at arrival or Crew&Pax at arrival, and from the departure notification if the request is for Hazmat at departure or Crew&Pax at departure. - WasteInformation and SecurityInformation from the arrival notification. - HazmatInformation from the arrival or departure notification depending on the value of GetHazmatType. - CrewAndPaxInformation from the arrival or departure notification depending on the value of GetCrewAndPaxType. The value of the APPLICATION_PARAMETER for sending CrewAndPax info to SSN is set to "activate". The system prepares the response with the corresponding ship call data	

	and marshals the MS2SSN_ShipCall_Res message.
Step 5	The message is send to SSN Central.
Use Case Description	Alternative Use Case scenario 2: (Internal error)
Step 1.1	The SSN Central has sent a valid request for information (SSN2MS_ShipCall_Req with From=”SSN”).
Step 1.2	The System identifies the request parameters: ShipCallResp – GetHazmat (optional) – GetWaste (optional) – GetSecurity (optional) – GetCrewAndPax (optional) AdditionalSearchCriteria – ShipCallId (mandatory) – GetHazmatType (optional) – GetCrewAndPaxType (optional)
Step 1.3	Searches the database for a relevant ship call (based on the ShipCallId which shall match the Journal Number of an existing ship call previously reported to SSN Central).
Step 1.4	An internal error prevents the system from preparing a response. The system prepares a response with StatusCode=”ServerError” and marshals the MS2SSN_ShipCall_Res message.
Step 1.5	The message is send to SSN Central.
Use Case Description	Alternative Use Case scenario 3: (Not Found)
Step 1.1	The SSN Central has sent a valid request for information (SSN2MS_ShipCall_Req with From=”SSN”).
Step 1.2	The System identifies the request parameters: ShipCallResp – GetCrewAndPax AdditionalSearchCriteria – ShipCallId – GetCrewAndPaxType
Step 1.3	Searches the database for the value of the APPLICATION_PARAMETER for sending CrewAndPax info to SSN. The value is set to “deactivate”.
Step 1.4	The system prepares a response with StatusCode=”NotFound” and marshals the MS2SSN_ShipCall_Res message.
Step 1.5	The message is send to SSN Central.
Input(s)	Request specific data.
Output(s)	Notification Details are sent to the SSN Central in case of no internal

	error.
Timer(s)	-
Business Process(es) Reference	-
Associated Use Case(s)	-
Special Requirements	-

Use Case Req ID	**UC-CDP-8**	
Use Case Name	**Routing request to Authorities**	
Purpose	The current use case describes the functionality of the Common Reporting Gateway related to the transmission of a clearance request to the Authorities Info Exchange.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	N/A	
Precondition(s)	A clearance notification is received by the ship data provider and is successfully validated by the Common Reporting Gateway, correlation with existing ship call is done.	
Postcondition(s)	A clearance request is pushed to the Authorities Info Exchange subsystem.	
Trigger(s)	System request via the extended Case: UC-CDP-4: Process clearance notification data. More specifically, a data event has taken place, namely the receipt of a notification.	
Input(s)	Corresponding data elements to the Arrival or Departure request for clearance. The consolidated data set for a given ship call is provided to the Authority Info Exchange.	
Output(s)	A clearance request is registered in the Authority Info Exchange data store.	
Timer(s)	-	
Business Process(es) Reference	N/A	
Associated Use Case(s)	Process Clearance data routing	
Special Requirements	N/A	

3.2.1.3 Send acknowledgement

This system package includes the services required by the NSW for the provision of clearance request information to the authorities, recording of their decision and the acknowledgement of a request. More specifically, this system package consists of the following use-cases:

1. UC-ACK-9: Provide Clearance information to authorities
2. UC-ACK-10: Register decision

3. UC-ACK-11: Send Acknowledgment
4. UC-ACK-12: Consult Acknowledgement

Use Case Req ID	**UC-ACK-9**
Use Case Name	**Provide Clearance information to authorities**
Purpose	The current use case describes the functionality related to the provision of Ship Call information to Authorities based on the distribution rules.
Subsystem	Authority Info Exchange
Primary Actor(s)	Authority
Precondition(s)	A clearance notification is successfully received, processed by the Common Reporting Gateway and consolidated into a Ship Call.
Postcondition(s)	Relevant information from the Ship Call is available to Authorities based on the configured access rights.
Trigger(s)	System request via the extended Case: UC-CDP-4: Process clearance notification data. More specifically, a data event has taken place, namely the receipt of a notification.
Use Case Description	Primary Workflow
Step 1	The Authority Info Exchange receives the Ship Call data object from the Common Reporting Gateway.
Step 2	Information received is parsed.
Step 3	Information is registered in the Authority Info Exchange data store: – If the Journal Number of the Ship Call is not already registered in the AIE, a new Ship Call is registered. – If the Journal Number of the Ship Call is already registered in the AIE, then the Ship Call information received replaces the existing Ship Call data. All decisions by each authority recorded with this Ship Call are changed to "Pending".
Step 4	Check configured tasks to identify the authorities which are relevant to the Ship Call and to which data must be provided. Relevant Authorities to a Ship Call are the Authorities which are assigned at least one CLEARANCE task which complies to the following (Business rule #31): - The task is related to a data group included in the Ship Call, and - The geographical scope of the task includes the Port of Call of the Ship Call.
Step 5	Send email message to the concerned authorities (which user account has emails enabled) to signal new/updated clearance request for a given ship, port of call and arrival/departure. A direct link will enable the user to direct to the corresponding AIE web page. Note: the user will need to provide his/her credentials to login the Web Application to access the information. Produce a signal on the Web Application for the concerned user (Authority); the signal will alert the user that new/updated clearance

	request is available.
Input(s)	The consolidated data set for a given Ship Call is provided to the Authority Info Exchange.
Output(s)	The user (authority relevant to the Ship Call) receives an alert via the web application and/or via email that new information are available for him/her.
Timer(s)	-
Business Process(es) Reference	Distribution rules are based on access right granted to the Authority depending on access rights configured per NSW by the National Administrator:
Associated Use Case(s)	-
Special Requirements	The user is required to access the Web application to access the information made available to him.

Use Case Req ID	**UC-ACK-10**	
Use Case Name	**Register decision**	
Purpose	The current use case describes the functionality of the Authority Info Exchange to register decision regarding a Ship Call by an Authority. Independent of the clearance model adopted by the NSW, the Authority Info Exchange will always communicate to the Common Reporting Gateway its decision on the clearance request. It is therefore up to the Common Reporting Gateway to process the acknowledgment message based on the clearance model. Clearance is recorded for all the data groups in the web application tab. The tasks required for an authority to give clearance per tab are: Tab "Port Call", "Voyage" and "PSC" : PORT_CALL_CLEARANCE Tab "Cargo" – Cargo specific data: CARGO_CLEARANCE. Tab "Cargo" – DPG specific data: DPG_CLEARANCE. Tab "Ship's Stores": SHIP_STORES_CLEARANCE Tab "Waste": WASTE_CLEARANCE Tab "Waste Receipt": WASTE_RECEIPT_CLEARANCE Tab "Security": SECURITY_CLEARANCE Tab "Crew" and "Passengers": CREW_AND_PASSENGERS_CLEARANCE Tab "Crew effects": CREW_EFFECTS_CLEARANCE Tab "Health": HEALTH_CLEARANCE. Tab "Other" – group "Bunkers remaining on-board": BUNKERS_CLEARANCE. Tab "Other" – groups "Civil Liability Certificate for Oil Pollution Damage"	

	and "Civil Liability Certificate for Bunker Oil Pollution Damage": LIABILITY_CERTIFICATES_CLEARANCE. Tab "Other" – group "Ship defects": SHIP_DEFECTS_CLEARANCE In addition the authority with a task "_CONSULT" will be able to view the data of the corresponding data group. Consult allows only to view data and not to provide clearance.
Subsystem	Authority Info Exchange
Primary Actor(s)	Authority
Precondition(s)	A Ship Call is successfully received and processed by the Authority Info Exchange. The Authority is assigned at least one "CLEARANCE" task.
Postcondition(s)	Any decision is recorded in the Authority Info Exchange along with the Ship Call and transmitted to the Common Reporting Gateway.
Trigger(s)	The user received an email alert or got the signal from the Web application that a new/updated clearance request is submitted and he/she has something to do. Alternatively the user search via the Web application for new notification that he/she has something to do.
Use Case Description	Primary Workflow: [Authority has taken a negative decision]
Step 1	The user directs to the Approve Notifications page; the page opens and the list of notifications is displayed. The list of notifications is filtered based on the user's default filter parameters. The user may filter the list of notifications based on Ship Name, IMO Number, MMSI Number, Port Of Call, Date (ETA/ATA for arrival notifications, ETD/ATD for departure notifications within 24H, 48H or 7 days), Ship Call Type, Ship Call Status, Request Status, and receives the Ship Calls for which he is a relevant Authority (Business rule #31). The list will display per Ship Call all the columns mentioned above as search criteria and an additional column named Formalities (icons of the EPC notification tabs for which data is reported). The filter parameters are stored primarily in the user's session and are persisted in the data store, along the user preferences (i.e. Language), at user logout. The user may click on the "Default filter" button to restore the default filter parameters. User can select per Ship Call to: • View notification history • View decisions (same as in step 3). • Record decision (same as in step 3). • Show ship on map. It will direct the user to the NSW GI interface and display the ship track on the map. If a Ship Call has a Ship Call status "Closed" or "Cancelled", it is displayed but the user cannot proceed to Step 2.
Step 2	Select a Ship Call and click on the "Record decision" button. The Web application displays the data groups of the selected Ship Call

	which are relevant to the Authority (Business Rule #33), including links to download the attached files associated with the data groups, along with the decisions and comments already recorded by this Authority (if any).
Step 3	The user reviews the information and records or updates his/her decision(s) and comments. The decision is that a data group of the Ship Call is Not Accepted. The user can select the corresponding button to view in a new web page the: – Notification History per user and date/Time – Decisions from each Authority per Authority (with indication of Authority's, name and agency(ies)), Data group, Date-time, Decision and Comments.
Step 4	The system then creates an Acknowledgement message and transmits the decision of the authority for a given data group or a set of data groups to the Common Reporting gateway. The Acknowledgment is given the Request Status = "NotAccepted".(Business rule #36)
Use Case Description	Alternative Scenario 1: [Authority has taken positive decision]
Step 1.1	Repeat step 1.
Step 1.2	Repeat step 2
Step 1.3	The user reviews the information and records or updates his/her decision(s) and possible comments. The decision is that a data group of the Ship Call is accepted. The user can select the corresponding button to view in a new web page the: – Notification History per user and date/Time – Decisions from each Authority Agency per Data group with indication of the Date-time, Decision and Comments.
Step 1.4	The system will then create an Acknowledgement message and transmits the decision of the authority for a given data group or a set of data groups to the Common Reporting gateway. The Acknowledgment is given Request Status = "Accepted". (Business rule #37).
Input(s)	Consolidated Ship Call and decisions already registered.
Output(s)	The Acknowledgement is propagated to the Common Reporting gateway.
Timer(s)	-
Business Process(es) Reference	Acknowledgement
Associated Use Case(s)	-

Special Requirements	An individual decision is recorded for a single data group and for a single Authority. An Authority may therefore record several decisions for a Ship Call. An Acknowledgment is recorded for each relevant Authority. A Ship Call may therefore have several Acknowledgments.

Use Case Req ID	**UC-ACK-11**	
Use Case Name	**Send Acknowledgment**	
Purpose	The current use case describes the functionality related to sending an Acknowledgment message to the Ship Data Provider(s). Sending an Acknowledgement depends on the clearance model adopted by the NSW: – No clearance: the NSW does not provide acknowledgement messages. Communication of the clearance decision is done outside of the NSW. – Silent clearance: The NSW only communicates acknowledgement messages to the ship data provider in the case where the clearance is denied or additional information is needed. The ship is considered by default as cleared once the notification is received by the NSW (positive receipt). – Systematic clearance: a clearance decision is always provided after reception of a notification by the NSW (positive receipt). The approval of clearance is consolidated before being communicated to the ship data provider. Based on the overall Request Status (as defined in section 3.1.1). The possible values for the Request status are defined in section 3.1.1.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	Ship Data Provider	
Precondition(s)	A clearance request has been processed by an Authority. The decision and comments are consolidated in the AIE in an Acknowledgment which is propagated to the CRG.	
Postcondition(s)	Any decision is recorded in Common Reporting Gateway along with the clearance notification request.	
Trigger(s)	An Acknowledgment is received by the CRG from the AIE.	
Use Case Description	Primary Workflow: [Systematic clearance model]	
Step 1	Parse and record the Acknowledgement. Define the Request Status of the notification See Business Rule n°42: • If there is at least one acknowledgment with Request Status "Not accepted", then the overall Request Status of the notification will be "Not accepted". • If there is no acknowledgment with Request Status "Not accepted", the system will consider the Agencies linked to authority users who are relevant for the notification (as defined	

	in business rule n° 31). If for each agency, there is at least one associated Acknowledgment with Request Status “Accepted”, then the overall Request Status of the notification will be “Accepted”. • In all other situations, the overall Request Status of the notification will be “Pending”.
Step 2	Check the adopted clearance model of the NSW. It is found to be “Systematic clearance” model.
Step 3	Marshal the Acknowledgement message. This will generate the XML message.
Step 4	If an Acknowledgment is received by the CRG with Request Status “NotAccepted” then send the acknowledgment to the Ship Data Providers who have successfully submitted a notification for this Ship Call. If an Acknowledgment is received by the CRG with Request Status “Accepted” and the Request Status of the notification in the CRG is “Accepted”, then send the acknowledgment to the Ship Data Providers who have successfully submitted a notification for this Ship Call
Use Case Description	Alternative Scenario 1: [Silent clearance model]
Step 1.1	Parse the Acknowledgement decision.
Step 1.2	Check the adopted clearance model. It is found to be “Silent clearance” model.
Step 1.3a	Marshal the Acknowledgement message in case of negative response.
Step 1.4a	In case the acknowledgment’s Request Status = “NotAccepted”, send the Acknowledgment to the Ship Data Providers who have successfully submitted a notification for this Ship Call.
Step 1.4b	In case the acknowledgment’s Request Status = “Accepted”, do nothing.
Use Case Description	Alternative Scenario 2: [No clearance model]
Step 2.1	Parse and record the Acknowledgement decision.
Step 2.2	Check the adopted clearance model. It is found to be “No clearance” model.
Step 2.3	This step is not executed.
Step 2.4	This step is not executed.
Input(s)	An Acknowledgement with decisions and comments from an Authority received by the CRG from the AIE
Output(s)	The Acknowledgement decision is recorded and depending on the clearance model adopted an Acknowledgment message is sent to the Ship data Provider. Message is send via the protocol the clearance notification was originally submitted (i.e. XML/Web).
Timer(s)	-

Business Process(es) Reference	Acknowledgement
Associated Use Case(s)	– Extended Case: UC-ACK-9: Provide Clearance information to authorities – Extended Case: UC-ACK-10: Register decision
Special Requirements	The clearance model shall be configurable per NSW. The application parameter CLEARANCE_MODEL shall be set to – No clearance or – Silent clearance or – Systematic clearance. An Acknowledgment is recorded for an individual Authority. A Ship Call may therefore have several Acknowledgments.

Use Case Req ID	**UC-ACK-12**	
Use Case Name	**Consult my notifications**	
Purpose	The current use case describes the functionality related to the display of all Ship Calls for which the user has contributed to and to the consultation of an Acknowledgment from authorities.	
Subsystem	Common Reporting Gateway	
Primary Actor(s)	Ship Data Provider	
Precondition(s)	The user must have a valid account and access rights to submit a clearance request. Moreover the user has previously sent at least one notification.	
Postcondition(s)	-	
Trigger(s)	-	
Use Case Description	Primary Workflow: [Consult my notifications]	
Step 1	The Actor is provided with a list of Ship Calls for which he has at least successfully submitted one notification. The Ship Calls can be filtered by Ship Name, IMO Number, Port of call, ETA/ATA (filter Ship Calls with ETA/ATA greater than or equal to the date entered by the user as criteria), Ship Call Type, Ship Call Status. The list displays the Ship Calls per IMO Number, Ship Name, MMSI Number, Port of call, Date (ETA/ATA for arrival notifications, ETD/ATD for departure notifications within 24H, 48H or 7 days), Ship Call type, Ship Call Status and Request Status.	
Step 2	Select one of the options: a) View acknowledgements. The Actor selects the desired Ship Call to view the decisions from each authority received so far. b) Create a new notification from an existing ship call. c) Send an update notification.	

	d) Send a new departure notification from arrival ship call. e) Send a new notification from the start.
Step 3.a	The application retrieves the Acknowledgement messages which were sent by the AIE to the CRG for that ship call and displays the list of relevant authorities and the content of associated Acknowledgment messages (Authority, Agency, Date-time, decisions and comments per Data Group)
Step 3.b,c,d,e	Proceed as in UC-RCNWEB-2 from Step 4 onwards.
Step 4	The user may press the Back button to return to the previous page.
Input(s)	The Acknowledgement messages with the decision and comments – consolidated per Authority - as sent by the AIE to the CRG.
Output(s)	The list or relevant Authorities and content of the Acknowledgement messages.
Timer(s)	-
Business Process(es) Reference	Acknowledgement. Process Clearance Notification via Web.
Associated Use Case(s)	– Included Case: UC-CDP-4: Process clearance notification data
Special Requirements	-

3.2.1.4 Configuration and resource management

This system package includes the services required by the NSW for the registration of users the configuration of regulatory information and the management of system resources such as users, ships and locations. More specifically, this system package consists of the following use-cases:

1. UC-CRM-13: Configure regulatory information
2. UC-CRM-14: Register to NSW
3. UC-CRM-15: Manage users
4. UC-CRM-16: Configure access rights
5. UC-CRM-17: Manage ships
6. UC-CRM-18: Manage shipping companies
7. UC-CRM-19: Manage locations
8. UC-CRM-20: Manage agencies
9. UC-CRM-21: Get Locations from SSN
10. UC-CRM-22: Get Ships from SSN
11. UC-CRM-23: Manage attachment types

Use Case Req ID	**UC-CRM-13**	
Use Case Name	**Configure regulatory information**	
Purpose	The current use case describes the system's functionality related to the configuration of regulatory information. A national administrator may configure the data elements of interest for the NSW. The configuration is stored as metadata in the NSW and defines the data model for the submission of clearance notifications to the NSW via XML/Web. It should be noted that the formalities, elements are restricted to those identified to be part of the current system specifications and must adhere to the mandatory elements business rules per formality as the minimum requirements according to the regulation. The aim is to provide the ship data providers a unified interface for reporting formalities; as such the configuration refers not to the definition of the clearance notifications but the formalities and data elements per formality each MS will utilise for the clearance process.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	The supporting markup definition for the distribution of the clearance requests is pre-defined.	
Postcondition(s)	The Common Reporting Gateway supporting data model is defined based on the configuration of regulatory information.	
Trigger(s)	The National administrator selects the Regulatory information management function available via the web interface.	
Input(s)	Formalities and data elements per formality as defined in the Master file (ref: [R11]).	
Output(s)	The activated data elements of the selected formalities of interest are defined in the data store.	
Timer(s)	-	
Business Process(es) Reference	The groups of data elements must be distinctively identified.	
Associated Use Case(s)	-	
Special Requirements	The RC will provide 2 lists: the first with the formalities and the second with the data elements. Each item in the lists will have a check box next to it. If the user selects a formality (check box checked) the system will automatically select (check) all the data elements of that formality. The formalities from legal acts of the Union (refer to formalities "A1 – Port" to "A5 – Security" of the Master File) will be checked by default and cannot be unchecked. For data elements common to several of the above formalities, if one or more of the corresponding formalities is activated, then the data element will be activated. The user will be able to further customise the list of checked data elements by selecting/de-selecting them. Only data elements which	

	are not mandatory (according to the Master File, column "Supported by all NSWs as reporting formality") may be unchecked by the user. When an individual element is manually unchecked, the formalities which include this element and which were selected get a visual indication that they are customised.

Use Case Req ID	**UC-CRM-14**	
Use Case Name	**Register to NSW**	
Purpose	The current use case describes the system's functionality related to a request by a new user for an account to access the NSW. The request is submitted to the National administrator for acceptance.	
Subsystems	Resource Management	
Primary Actor(s)	Ship data provider Authority National Administrator	
Precondition(s)	N/A	
Postcondition(s)	A request for a new user account is recorded in NSW.	
Trigger(s)	The user via either the Common Reporting gateway or the Authority Info Exchange web site registers a request for a new user account.	
Input(s)	User specific information such as: – Profile: ship data provider/authority. Profile is defined automatically whether the request is made through the Common Reporting Gateway or the Authority Info Exchange. – First and last names; – Organization the user belongs to; – Function(s) performed; – In the case of a Ship Data Provider: indication of the associated country (name of company agency) – Email account; – Preferred user_id and password.	
Output(s)	The NSW records the request and prompts the National Administrator via the web interface (alert) and/or email.	
Timer(s)	-	
Business Process(es) Reference	The user details must be filled in. Verification of the user data shall be performed by the National administrator in charge. Once verified and approved the National administrator completes the user registration by granting access to concerned functionalities and communicates the decision to the user via email. The email contains all user details and the URI to the preferred NSW interface.	

	In case of a web the user must reset his/her password and accept the rules and condition of usage prior to entering the application.
Associated Use Case(s)	-
Special Requirements	N/A

Use Case Req ID	**UC-CRM-15**	
Use Case Name	**Manage users**	
Purpose	The current use case describes the system's functionality related to management of user accounts. Both Web users and external systems interface with the NSW share common characteristics; as such their management could be handled by the same set of web pages.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	N/A	
Postcondition(s)	User/external system definition data are recorder in the NSW.	
Trigger(s)	The National administrator selects the User management function available via the Web interface.	
Use Case Description	Primary Workflow: [Create new user]	
Step 1	Select the new user function.	
Step 2	Define: – A unique user ID and password. – Contact person details (given name, family name, phone, fax, , email etc). – If the account is enabled and, if provided, until which date the account is enabled. – If the user will receive email notifications – The agency (ies) the user is associated with, from the list of agencies displayed by Name. (mandatory) – Preferred interface: XML/SOAP or Web. – In case of XML the URI for message transmissions. – Assign the profile (Ship data provider/Authority/National Administrator). – Once the profile is selected the list of permitted tasks is populated. By default all the tasks in the profile are assigned to the user. The geographical restriction (where applicable) is the default defined for the profile. – Deselect any tasks to revoke access. – Change the default geographical restriction if necessary.	

Step 3	Submit new user account details.
Step 4	The system validates data entered: – If valid the new user is registered in the data store. The created by and created on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 3.
Use Case Description	Alternative Scenario 1: [Update existing user]
Step 1.1	Select the update user function.
Step 1.2	Search for a user account by its userId, family name, given name, agency, status (enabled/disabled/all, with "enabled" selected by default) or profile (with "all" selected by default). From the result list select the user account to update. If no results the admin shall modify the search criteria.
Step 1.3	Update any of the below mentioned: – The password. – Contact person details (given name, family name, phone, fax, email etc). – The agency (ies) the user represents/acts on behalf (in case of ship data provider), from the list of agencydisplayed by Name and IMO Number. – Preferred interface: XML/SOAP or Web. – In case of XML the URI for message transmissions. – Select or Deselect tasks to grant/revoke access respectively. – Change the default geographical restriction if necessary.
Step 1.4	Submit updated user account details.
Step 1.5	The system validates data entered: – If valid the updated user is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 1.4.
Input(s)	Distinction to actor and assignment of a profile: Ship data provider/Authority/National Administrator (in case more than one person is assigned this task). User_id that uniquely identified the user/external system. Contact person details (including email which is mandatory for the propagation of email alert messages). Preferred interface: XML/SOAP or Web. In case of XML the URI for message transmissions. Every group of data elements is linked to a pre-defined task. The tasks are assigned to profiles that in turn are assigned to users. One that is assigned a profile with a task can perform the function

	related with that task. One can be assigned one or more tasks. Every task is unique.
Output(s)	The user account is registered in the data store.
Timer(s)	-
Business Process(es) Reference	A user must be uniquely identified by the user_id to be provided in all communications to/from NSW. An external system must have a specific interface that communicates with NSW. A user/external system must have a pre-defined profile assigned to access information communicated via NSW. Access to the management of resources is restricted to the National administrator profile. User data updates are recorded for monitoring purposes in the database (i.e. user performing an action, date/time of action performed.)
Associated Use Case(s)	includedCase: UC-CRM-14: Register to NSW
Special Requirements	N/A

Use Case Req ID	**UC-CRM-16**	
Use Case Name	**Configure access rights**	
Purpose	The current use case describes the system's functionality related to the configuration of access rights. Access rights are defined based on a task the user is granted (refer to Annex B: Profiles and Tasks). While the set of data groups are pre-defined the UC-CRM-13: Configure regulatory information will define the groups that are of interest to the NSW. The list of groups of interest defines the set of tasks applicable for the NSW. Tasks are assigned to profiles. The profile is then assigned to a user. The user is then restricted to the list of tasks assigned to his/her profile. The set of profiles can be extended to the default set of Ship Data Provider, Authority and National Administrator.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	UC-CRM-13: Configure regulatory information Alternatively the full set of Tasks will be considered.	
Postcondition(s)	Task assignment to profiles.	
Trigger(s)	The National administrator selects the Configure access right function available via the Web interface.	
Use Case Description	Primary Workflow: [Configure access rights]	
Step 1	Select a profile.	

Step 2	The profile is displayed along with the list of predefined tasks. Per task the default geographical restriction is also defined. Tasks assigned to a profile are checked. Tasks not assigned are unchecked. Check or uncheck from the list of tasks. Per task, change the default geographical restriction (choices are Country, Area and Locodes). Per task, indicate if the function is restricted for the agency the user represents/acts on behalf.
Step 3	Submit updated profile.
Step 4	The system validates data entered: – If valid the updated profile is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 3.
Input(s)	A predefined list of tasks. The default set of profiles.
Output(s)	The profile is updated with the list of tasks assigned to it.
Timer(s)	-
Business Process(es) Reference	A profile must be uniquely identified. A task can be assigned to a profile only once. A task can be assigned to more than one profile. Please refer to Annex B: Profiles and Tasks for the list of profiles and tasks.
Associated Use Case(s)	-
Special Requirements	N/A

Use Case Req ID	**UC-CRM-17**	
Use Case Name	**Manage ships**	
Purpose	The current use case describes the system's functionality related to the management of ships.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	-	
Postcondition(s)	Ship definition data are registered in the NSW.	
Trigger(s)	The National administrator selects the Ship data management function available via the web interface.	
Use Case Description	Primary Workflow: [Create new ship]	

Step 1	Select the new ship function.
Step 2	Define: – IMO Number (mandatory, cannot be an IMO number already recorded) – MMSI Number, Name and Call Sign. – Comment – Flag State – Certificate of registry – Port, Date and Number – Inmarsat call number – Gross tonnage – Net tonnage – Type – Year of built – Dead Weight – Length Overall – Beam Select the shipping company of the vessel from the list of shipping companies displayed by Name and IMO Number.
Step 3	Submit new ship details.
Step 4	The system validates data entered: – If valid the new ship is registered in the data store. The created by and created on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 3.
Step 5	The system generates a MS2SSN_ShipParticulars_Not.xml. The notification will report to SafeSeaNet the new ship identified by its IMONumber. The following particulars will be provided: CallSign, ShipName, Flag, Inmarsat call number (use the first), GrossTonage, NetTonage, Type (ShipType_UN in CSD), Year of built (Keel-laying_Date in CSD), DeadWeight, LengthOverall (length in CSD) and Beam. The date of effect=currentTimestamp. The reason for update will be "UP_MS_VERIFIED". The notification will be transmitted to SafeSeaNet.
Use Case Description	Alternative Scenario 1: [Update existing ship]
Step 1.1	Select the update ship function.
Step 1.2	Search for a ship by its IMO Number, MMSI Number, Ship Call, Ship Name. From the result list select the ship to update. If no results the admin shall modify the search criteria.
Step 1.3	Update any of the below mentioned: – MMSI Number, Ship Call and Call Sign.

	– Comment – Flag State – Certificate of registry – Port, Date and Number – Inmarsat call number – Gross tonnage – Net tonnage – Ship type – The shipping company of the vessel from the list of shipping companies displayed by Name and IMO Number.
Step 1.4	Submit updated ship details.
Step 1.5	The system validates data entered: – If valid the updated ship is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 1.4.
Step 5	The system generates a MS2SSN_ShipParticulars_Not.xml. The notification will report to SafeSeaNet all the updated ship attributes and will be identified by its IMONumber. The date of effect=currentTimestamp. The reason for update will be "UP_MS_VERIFIED". The notification will be transmitted to SafeSeaNet.
Input(s)	Ship definition: 1. Ship identification (Ship IMO Number is mandatory) 2. Ship particulars
Output(s)	Ship definition registered in the data store.
Timer(s)	-
Business Process(es) Reference	A ship is uniquely identified by the IMO number. The National administrator has access to all ships. The list of ships can be edited by the admin to include more ships. Ship data updates are recorded for monitoring purposes in the database (i.e. user performing an action, date/time of action performed.)
Associated Use Case(s)	-
Special Requirements	Initial set of ship data will be provided by EMSA. Update of ship data can be done via clearance request notifications submitted provided the reported ship particulars are technically correct (ref: section 3.1). If a formality is notified to the NSW for a ship not in the ship database, the NSW automatically creates the ship. Ships without IMO Number will be recorded but considered as "not validated" (therefore functionalities would be limited because the ship is not identified).

Use Case Req ID	**UC-CRM-18**	
Use Case Name	**Manage shipping companies**	
Purpose	The current use case describes the system's functionality related to the management of shipping companies.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	N/A	
Postcondition(s)	Shipping company definition data are registered in the NSW.	
Trigger(s)	The National administrator selects the Ship company management function available via the web interface.	
Use Case Description	Primary Workflow: [Create new shipping company]	
Step 1	Select the new shipping company function.	
Step 2	Define: – Name of company – IMO company number – Country – Company's contact numbers – CSO name ○ Given name ○ Family name – CSO 24 hour contact details ○ Phone ○ Fax ○ Email	
Step 3	Submit new shipping company details.	
Step 4	The system validates data entered: – If valid the new shipping company is registered in the data store. The created by and created on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 3.	
Use Case Description	Alternative Scenario 1: [Update existing shipping company]	
Step 1.1	Select the update shipping company function.	
Step 1.2	Search for a shipping company by its IMO Number. From the result list select the shipping company to update. If no results the admin shall modify the search criteria.	
Step 1.3	Update any of the below mentioned: – Name of company – Country – Company's contact numbers – CSO name ○ Given name ○ Family name	

	– CSO 24 hour contact details ○ Phone ○ Fax ○ Email
Step 1.4	Submit updated shipping company details.
Step 1.5	The system validates data entered: – If valid the updated shipping company is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 1.4.
Input(s)	Shipping company Name, IMO number, country, contact numbers.
Output(s)	Shipping company definition registered in the data store.
Timer(s)	-
Business Process(es) Reference	A shipping company is uniquely identified by the IMO company number The National administrator has access to all shipping companies. The list of shipping companies can be edited by the admin to include more.
Associated Use Case(s)	-
Special Requirements	N/A

Use Case Req ID	**UC-CRM-19**	
Use Case Name	**Manage locations**	
Purpose	The current use case describes the system’s functionality related to the management of locations.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	The “Get locations from SafeSeaNet” service is inactive. If not then the system will not allow access to the manage locations web pages.	
Postcondition(s)	Location definition data are registered in the NSW.	
Trigger(s)	The National administrator selects the Location data management function available via the web interface.	
Use Case Description	Primary Workflow: [Create new location]	
Step 1	Select the new location function.	
Step 2	Define: – Locode = Country ISO 2-aplha code + UNLocode (Mandatory) – Name – Country (Mandatory) – Geographical coordinates: ○ Latitude	

	○ Longitude
Step 3	Submit new location details.
Step 4	The system validates data entered: – If valid the new location is registered in the data store. The created by and created on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 3.
Use Case Description	Alternative Scenario 1: [Update existing location]
Step 1.1	Select the update location function.
Step 1.2	Search for a location by its Name or Locode. From the result list select the location to update. If no results the admin shall modify the search criteria.
Step 1.3	Update any of the below mentioned: – Name – Country – Geographical coordinates: ○ Latitude ○ Longitude
Step 1.4	Submit updated location details.
Step 1.5	The system validates data entered: – If valid the updated location is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 1.4.
Input(s)	Location definition attributes.
Output(s)	Location definition registered in the data store.
Timer(s)	-
Business Process(es) Reference	A location is uniquely defined by its Locode. The National administrator has access to all locations. The list of locations can be edited by the admin to include more locations. Location data updates are recorded for monitoring purposes in the database (i.e. user performing an action, date/time of action performed.)
Associated Use Case(s)	-
Special Requirements	Initial set of locations data will be provided by EMSA.

Use Case Req ID	**UC-CRM-20**	
Use Case Name	**Manage agencies**	
Purpose	The current use case describes the system’s functionality related to the	

	management of agencies.
Subsystem	Resource Management
Primary Actor(s)	National Administrator
Precondition(s)	N/A
Postcondition(s)	Agency definition data are registered in the NSW.
Trigger(s)	The National administrator selects the Agency management function available via the web interface.
Use Case Description	Primary Workflow: [Create new agency]
Step 1	Select the new agency function.
Step 2	Define: – Name of agency (mandatory) – Business phone number – Fax number – Email
Step 3	Submit new agency details.
Step 4	The system validates data entered: – If valid the new agency is registered in the data store. The system trims the name and replaces multiple spaces by single spaces. The created by and created on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 3.
Use Case Description	Alternative Scenario 1: [Update existing agency]
Step 1.1	Select the update agency function.
Step 1.2	Search for an agency by its Name. From the result list select the agency to update. If no results the admin shall modify the search criteria.
Step 1.3	Update any of the below mentioned: – Name of agency – Business phone number – Fax number – Email
Step 1.4	Submit updated agency details.
Step 1.5	The system validates the record to ensure that the name is not already registered in the database (search is not case sensitive and not diacritic sensitive). The system validates data entered: – If valid the updated agency is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 1.4.
Input(s)	Agency Name and contact numbers.
Output(s)	Agency definition registered in the data store.

Timer(s)	-
Business Process(es) Reference	An agency is uniquely identified by the name. The National administrator has access to all agencies. The list of agencies can be edited by the admin to include more.
Associated Use Case(s)	-
Special Requirements	N/A

Use Case Req ID	**UC-CRM-21**	
Use Case Name	**Get Locations from SSN**	
Purpose	The current use case describes the system's functionality related to the request from the SSN Central Locations Database (CLD) of the list of Locations and the subscription to CLD service for a specific period to receive Location record updates.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	N/A	
Postcondition(s)	The NSW MNG_LOCATIONS database table is updated with data from the CLD.	
Trigger(s)	Actor submits a request manually via the web.	
Use Case Description	Primary Workflow: [Subscribe to the CLD location announcement request service]	
Step 1	The user selects the menu option Locations > "Get Locations from SafeSeaNet" to activate the homonymous web page.	
Step 2	Click on the checkbox "Get locations from SafeSeaNet" to activate. The system will prompt the user to confirm the selection made. Select the period (From – To) to subscribe to the CLD service to receive Location record updates. The timestamp of the last update is also displayed.	
Step 3	The application will generate: A MS2SSN_LocationAnn_Req message for all Countries and Application.ApplicationName = 'SSN'. In response the system will receive from the CLD the notifications with location record updates. The locations received will be merged with the locations defined in the MNG_LOCATIONS table. Criteria for the merge option will be the LOCODE. If a location is not found then it will be inserted; if found it will be updated.	
Step 4	The system will prompt the user to confirm the subscription was accepted based on the SSN_Receipt from SafeSeaNet.	
Use Case Description	Alternative Scenario 1: [Stop the CLD location announcement request service]	
Step 1.1	The user selects the menu option Ships > "Get Locations from	

	SafeSeaNet" to activate the homonymous web page.
Step 1.2	Uncheck the box "Get locations from SafeSeaNet". The system will prompt the user to confirm the selection made. The timestamp of the last update is also displayed.
Step 1.3	The application will stop processing the SSN2MS_LocationAnn_Res messages.
Step 1.4	The system will prompt the user to confirm the processing of CLD location announcement is stopped.
Use Case Description	Alternative Scenario 3: [Request MS2SSN_LocationAnn_Req registration fails]
Step 3.2	The application generate a MS2SSN_LocationAnn_Req message for all Countries and Application.ApplicationName = 'SSN'.
Step 3.3	The application receives an acknowledgement that the registration failed and prompts the user with the error message.
Input(s)	-
Output(s)	MNG_LOCATIONS database table is updated.
Timer(s)	-
Business Process(es) Reference	SSN Central identifies the Member State NSW as the CLD data requestor.
Associated Use Case(s)	-
Special Requirements	-

Use Case Req ID	**UC-CRM-22**	
Use Case Name	**Get Ships from SSN**	
Purpose	The current use case describes the system's functionality related to the request from the SSN Central Ships Database (CSD) of the list of Ships and the subscription to CSD service for a specific period to receive Ship record updates.	
Subsystem	Resource Management	
Primary Actor(s)	National Administrator	
Precondition(s)	N/A	
Postcondition(s)	The NSW MNG_SHIPS database table is updated with data from the CSD.	
Trigger(s)	Actor submits a request manually via the web.	
Use Case Description	Primary Workflow: [Subscribe to the CSD ship announcement request service]	
Step 1	The user selects the menu option Ships > "Get Ships from SafeSeaNet" to activate the homonymous web page.	
Step 2	Click on the checkbox "Get ships from SafeSeaNet" to activate. The	

	system will prompt the user to confirm the selection made. The timestamp of the last update is also displayed.
Step 3	The application will generate: A MS2SSN_ShipParticulars_Sub message. In response the system will receive from the CSD the notifications with ship record updates. The ships received will be merged with the ships defined in the MNG_SHIPS table. The attributes: MMSINumber, CallSign ShipName, Flag, Inmarsat call numbers, GrossTonage, NetTonage, Type (ShipType_UN in CSD), Year of built (Keel-laying_Date in CSD), DeadWeight, LengthOverall (length in CSD) and Beam will be considered. Criteria for the merge option will be the IMO Number. If a ship is not found then it will be inserted; if found it will be updated.
Step 4	The system will prompt the user to confirm the subscription was accepted based on the SSN_Receipt from SafeSeaNet.
Use Case Description	Alternative Scenario 1: [Un-subscribe from the CSD ship announcement request service].
Step 1.1	The user selects the menu option Ships > "Get Ships from SafeSeaNet" to activate the homonymous web page.
Step 1.2	Uncheck the box "Get ships from SafeSeaNet". The system will prompt the user to confirm the selection made.
Step 1.3	The application will generate: A MS2SSN_ShipParticulars_Sub message with element CancelSubscription > CancelDataPush = "Yes" and the MSRefID of the request subscription to cancel.
Step 1.4	The system will prompt the user to confirm the cancelation of the subscription was accepted based on the SSN_Receipt from SafeSeaNet.
Use Case Description	Alternative Scenario 3: [Request MS2SSN_ShipParticulars_Sub registration fails]
Step 3.2	The application generates a MS2SSN_ShipParticulars_Sub message.
Step 3.3	The application receives an acknowledgement that the registration failed and prompts the user with the error message.
Input(s)	-
Output(s)	MNG_SHIPS database table is updated.
Timer(s)	-
Business Process(es) Reference	SSN Central identifies the Member State NSW as the CSD data requestor.
Associated Use Case(s)	-
Special Requirements	-

Use Case Req ID	**UC-CRM-23**
Use Case Name	**Manage attachment types**
Purpose	The current use case describes the system’s functionality related to the management of attachment types.
Subsystem	Resource Management
Primary Actor(s)	National Administrator
Precondition(s)	N/A
Postcondition(s)	Attachment types definition data are registered in the NSW.
Trigger(s)	The National administrator selects the Attachment types function available via the web interface.
Use Case Description	Primary Workflow: [Create new attachment types]
Step 1	Select the new attachment types function.
Step 2	Define: – Name of attachment type (mandatory) – Data Group (mandatory)
Step 3	Submit new attachment type details.
Step 4	The system validates data entered: – If valid the new attachment type is registered in the data store. – If not the application prompts the admin with the error messages to correct before returning to step 3.
Use Case Description	Alternative Scenario 1: [Update existing attachment type]
Step 1.1	Select the update attachment type function.
Step 1.2	Search for an attachment type by its Name. From the result list select the attachment type to update. If no results the admin shall modify the search criteria.
Step 1.3	Update any of the below mentioned: – Name of attachment type (mandatory) – Data Group (mandatory)
Step 1.4	Submit updated attachment type details.
Step 1.5	The system validates the record to ensure that the name is not already registered in the database (search is not case sensitive and not diacritic sensitive). The system validates data entered: – If valid the updated attachment type is registered in the data store. The updated by and updated on info are stored along the new record. – If not the application prompts the admin with the error messages to correct before returning to step 1.4.
Input(s)	Attachment type Name and Data Group.
Output(s)	Attachment type definition registered in the data store.

Timer(s)	-
Business Process(es) Reference	An attachment type is uniquely identified by the name. The National administrator has access to all attachment type. The list of attachment type can be edited by the admin to include more.
Associated Use Case(s)	-
Special Requirements	N/A

4 Design of System Components

4.1 Overview

This section provides an overview of the NSW System. The SSN-EIS architecture shall not be changed as well as the communication protocols between the system components and the external systems.

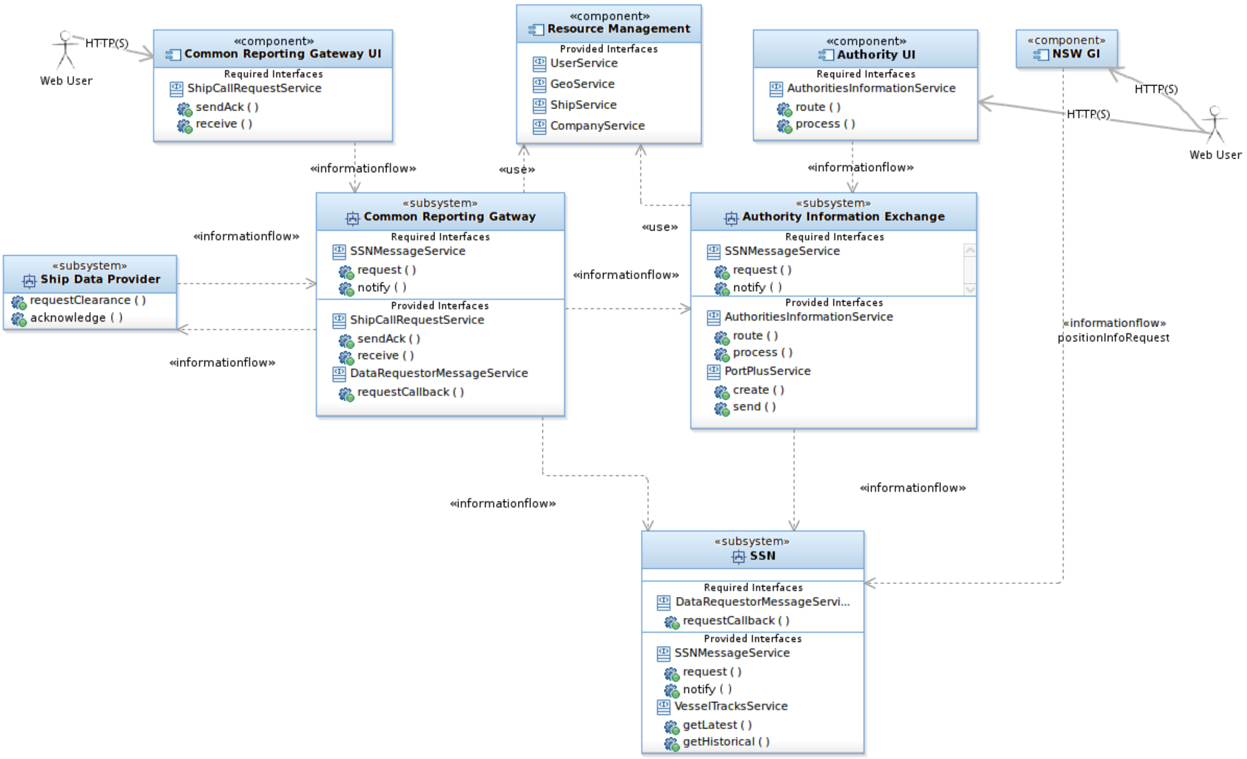


Figure 4-1 Component diagram of NSW system

NSW system consists of the following subsystems as depicted in Figure 4-1:

1. **Ship Data Provider** subsystem represents the external systems that submit requests for clearance to NSW and receive the acknowledgement messages related to the clearance process status. This communication is based on the NSW Message Services (nsw.wsdl) and the EPC XML schema (epc.xsd); this subsystem is out of the scope of this document.
2. **Common Reporting Gateway UI** component provides web interface for the aforementioned Ship Data Provider functionality. It also provides for the Port Clearance requests from SSN system for re-use of information via the Common Reporting Gateway subsystem.
3. **Common Reporting Gateway** subsystem provides an electronic interface between the ship or the ship representatives and authorities ashore. More specifically, it provides
    a. a reporting interface to ship data providers;

   b. a routing interface to delegate the information to the Authority Information Exchange, as well as the acknowledgement messages from authorities to the ship data providers to inform them on the clearance process status (this feature shall buffer and merge acknowledgements from two or more authorities so to send only one acknowledgement message to the ship);
   c. an email interface (via the container mail session) to alert Authorities when a new notification has been distributed to them.
   d. a Request/Response interface to receive ShipCall information from SSN system.
4. **Authority Information Exchange** subsystem provides
   a. the distribution of information reported in clearance requests from the ship data providers to the participant authorities. It manages the distribution of notifications information to national authorities in change as well as the grant/revocation/request for additional info to requests for clearance; additionally, it provides the acknowledge creation and distribution to the clearance requestors
   b. the creation of the revamped PortPlus notification and submission to the SSN Central.
5. **Authority UI** component provides web interface for the aforementioned NSW Core functionality related to authorities (4.a).
6. **Resource Management** component provides
   a. the users management as well as profiles and access rights management,
   b. reference data management including ships, shipping companies, countries, locations and other system resources.
7. This component is used by the aforementioned Common Reporting Gateway and NSW core subsystems. NSW-GI component provides a GIS web interface that presents AIS based position information of vessels in graphical form, overlaid on top of a digital map. The provided user interface complements those provided by the Common Reporting Gateway and Authority UI components, merging spatial information provided by SSN with ship-call information provided by NSW.
8. **SSN** subsystem represents the external EMSA SSN Centralised to exchange ShipCall and PortPlus information with NSW system. This communication is based on the SSN Message Services (messageservice.wsdl) and the corresponding SSN v2 XML schema (ssn.xsd) – this schema shall be extended to define the revamped PortPlus message; the architecture and design of this subsystem shall not modified and it is out of the scope of this document.

The NSW system is identified by the following entities owned by the "NSW Management" Business System

- Users; They are classified to Ship Data Providers / Authorities / National Administrators
- Ships
- Shipping companies
- Countries / Locations
- ShipCall Request / Response information exchanged with SSN System
- Port Clearance information that includes the above entities
- PortPlus notification that is created from the Port Clearance information and sent to SSN System.

Thus, NSW system provides a number of web services that enable the access to, and update of, these entities as shown in Figure 4-2.

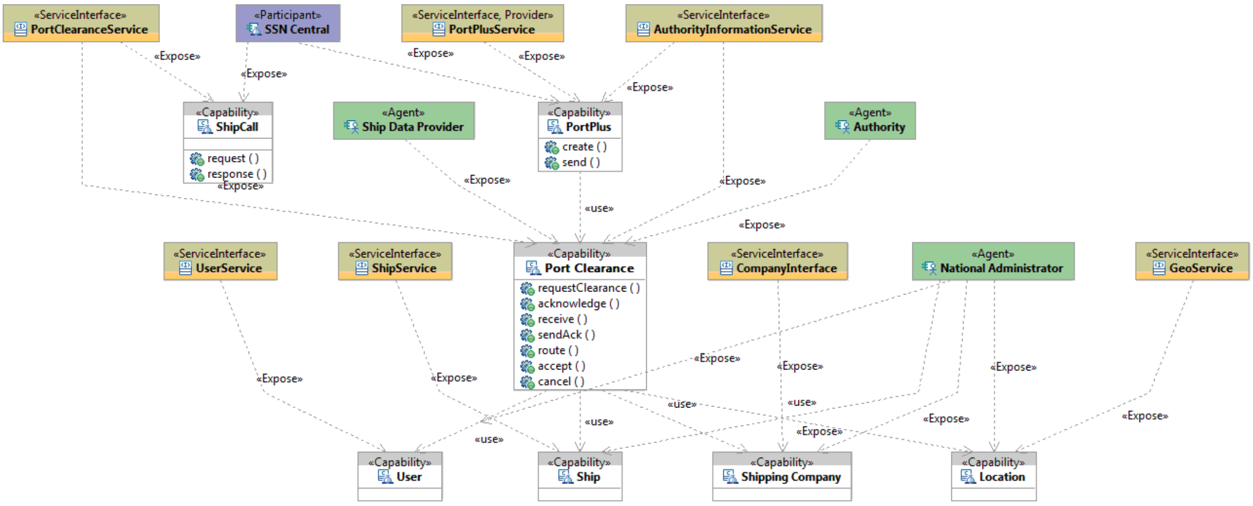

«ServiceInterface» PortClearanceService
«Participant» SSN Central
«ServiceInterface, Provider» PortPlusService
«ServiceInterface» AuthorityInformationService
«Capability» ShipCall
request ()
response ()
«Agent» Ship Data Provider
«Capability» PortPlus
create ()
send ()
«Agent» Authority
«ServiceInterface» UserService
«ServiceInterface» ShipService
«Capability» Port Clearance
requestClearance ()
acknowledge ()
receive ()
sendAck ()
route ()
accept ()
cancel ()
«ServiceInterface» CompanyInterface
«Agent» National Administrator
«ServiceInterface» GeoService
«Capability» User
«Capability» Ship
«Capability» Shipping Company
«Capability» Location
«Expose»
«use»

Figure 4-2 NSW Services provided operations.

4.2 NSW Common modules

4.2.1 Domain module/package

This module contains the domain model; the data object. This module is used by all the other modules of NSW system.

It includes the definition of NSW entities (PortClearance, ship, shipping company, location, user etc) with respect to epc.xsd and SSN entities (ShipCall, PortPlus) with respect to ssn.xsd.

4.2.1.1 UML Class Diagrams

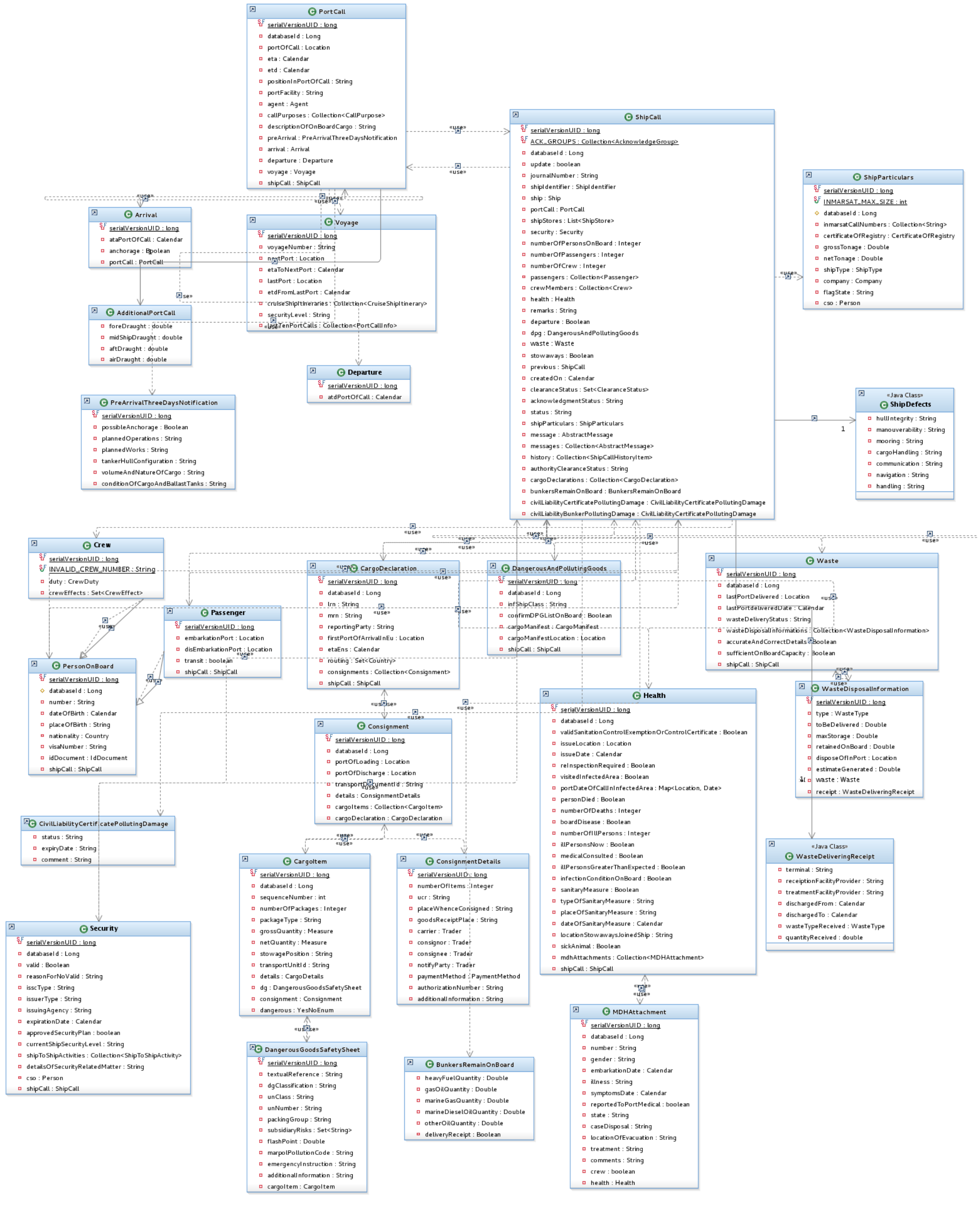
This section covers the architectural significant elements of the design model. It presents the definition of the most significant classes that will implement the requested functionality, organised into packages.

The classes are organised in packages according to the functionality they provide. A package is a general-purpose model element that organizes model elements into groups. Each package contains a set of classes and interfaces, representing what will become components in the implementation.

4.2.1.2 Module: nsw-domain

4.2.1.2.1 Package: emsa.nsw.domain

Class Diagram : port clearance request


PortCall
serialVersionUID : long
databaseId : Long
portOfCall : Location
eta : Calendar
etd : Calendar
positionInPortOfCall : String
portFacility : String
agent : Agent
callPurposes : Collection<CallPurpose>
descriptionOfOnBoardCargo : String
preArrival : PreArrivalThreeDaysNotification
arrival : Arrival
departure : Departure
voyage : Voyage
shipCall : ShipCall
«use»
Arrival
serialVersionUID : long
ataPortOfCall : Calendar
anchorage : Boolean
portCall : PortCall
Voyage
serialVersionUID : long
voyageNumber : String
nextPort : Location
etaToNextPort : Calendar
lastPort : Location
etdFromLastPort : Calendar
cruiseShipItineraries : Collection<CruiseShipItinerary>
securityLevel : String
lastTenPortCalls : Collection<PortCallInfo>
AdditionalPortCall
foreDraught : double
midShipDraught : double
aftDraught : double
airDraught : double
Departure
serialVersionUID : long
atdPortOfCall : Calendar
PreArrivalThreeDaysNotification
serialVersionUID : long
possibleAnchorage : Boolean
plannedOperations : String
plannedWorks : String
tankerHullConfiguration : String
volumeAndNatureOfCargo : String
conditionOfCargoAndBallastTanks : String
ShipCall
serialVersionUID : long
ACK_GROUPS : Collection<AcknowledgeGroup>
databaseId : Long
update : boolean
journalNumber : String
shipIdentifier : ShipIdentifier
ship : Ship
portCall : PortCall
shipStores : List<ShipStore>
security : Security
numberOfPersonsOnBoard : Integer
numberOfPassengers : Integer
numberOfCrew : Integer
passengers : Collection<Passenger>
crewMembers : Collection<Crew>
health : Health
remarks : String
departure : Boolean
dpg : DangerousAndPollutingGoods
waste : Waste
stowaways : Boolean
previous : ShipCall
createdOn : Calendar
clearanceStatus : Set<ClearanceStatus>
acknowledgmentStatus : String
status : String
shipParticulars : ShipParticulars
message : AbstractMessage
messages : Collection<AbstractMessage>
history : Collection<ShipCallHistoryItem>
authorityClearanceStatus : String
cargoDeclarations : Collection<CargoDeclaration>
bunkersRemainOnBoard : BunkersRemainOnBoard
civilLiabilityCertificatePollutingDamage : CivilLiabilityCertificatePollutingDamage
civilLiabilityBunkerPollutingDamage : CivilLiabilityCertificatePollutingDamage
ShipParticulars
serialVersionUID : long
INMARSAT_MAX_SIZE : int
databaseId : Long
inmarsatCallNumbers : Collection<String>
certificateOfRegistry : CertificateOfRegistry
grossTonage : Double
netTonage : Double
shipType : ShipType
company : Company
flagState : String
cso : Person
«Java Class»
ShipDefects
hullIntegrity : String
manouverability : String
mooring : String
cargoHandling : String
communication : String
navigation : String
handling : String
1
Crew
serialVersionUID : long
INVALID_CREW_NUMBER : String
duty : CrewDuty
crewEffects : Set<CrewEffect>
Passenger
serialVersionUID : long
embarkationPort : Location
disEmbarkationPort : Location
transit : boolean
shipCall : ShipCall
PersonOnBoard
serialVersionUID : long
databaseId : Long
number : String
dateOfBirth : Calendar
placeOfBirth : String
nationality : Country
visaNumber : String
idDocument : IdDocument
shipCall : ShipCall
CargoDeclaration
serialVersionUID : long
databaseId : Long
lrn : String
mrn : String
reportingParty : String
firstPortOfArrivalInEu : Location
etaEns : Calendar
routing : Set<Country>
consignments : Collection<Consignment>
shipCall : ShipCall
DangerousAndPollutingGoods
serialVersionUID : long
databaseId : Long
infShipClass : String
confirmDPGListOnBoard : Boolean
cargoManifest : CargoManifest
cargoManifestLocation : Location
shipCall : ShipCall
Waste
serialVersionUID : long
databaseId : Long
lastPortDelivered : Location
lastPortdeliveredDate : Calendar
wasteDeliveryStatus : String
wasteDisposalInformations : Collection<WasteDisposalInformation>
accurateAndCorrectDetails : Boolean
sufficientOnBoardCapacity : Boolean
shipCall : ShipCall
WasteDisposalInformation
serialVersionUID : long
type : WasteType
toBeDelivered : Double
maxStorage : Double
retainedOnBoard : Double
disposeOfInPort : Location
estimateGenerated : Double
waste : Waste
receipt : WasteDeliveringReceipt
«Java Class»
WasteDeliveringReceipt
terminal : String
receiptionFacilityProvider : String
treatmentFacilityProvider : String
dischargedFrom : Calendar
dischargedTo : Calendar
wasteTypeReceived : WasteType
quantityReceived : double
Consignment
serialVersionUID : long
databaseId : Long
portOfLoading : Location
portOfDischarge : Location
transportDocumentId : String
details : ConsignmentDetails
cargoItems : Collection<CargoItem>
cargoDeclaration : CargoDeclaration
Health
serialVersionUID : long
databaseId : Long
validSanitationControlExemptionOrControlCertificate : Boolean
issueLocation : Location
issueDate : Calendar
reInspectionRequired : Boolean
visitedInfectedArea : Boolean
portDateOfCallInInfectedArea : Map<Location, Date>
personDied : Boolean
numberOfDeaths : Integer
boardDisease : Boolean
numberOfIllPersons : Integer
illPersonsNow : Boolean
medicalConsulted : Boolean
illPersonsGreaterThanExpected : Boolean
infectionConditionOnBoard : Boolean
sanitaryMeasure : Boolean
typeOfSanitaryMeasure : String
placeOfSanitaryMeasure : String
dateOfSanitaryMeasure : Calendar
locationStowawaysJoinedShip : String
sickAnimal : Boolean
mdhAttachments : Collection<MDHAttachment>
shipCall : ShipCall
CivilLiabilityCertificatePollutingDamage
status : String
expiryDate : String
comment : String
Security
serialVersionUID : long
databaseId : Long
valid : Boolean
reasonForNoValid : String
isscType : String
issuerType : String
issuingAgency : String
expirationDate : Calendar
approvedSecurityPlan : boolean
currentShipSecurityLevel : String
shipToShipActivities : Collection<ShipToShipActivity>
detailsOfSecurityRelatedMatter : String
cso : Person
shipCall : ShipCall
CargoItem
serialVersionUID : long
databaseId : Long
sequenceNumber : int
numberOfPackages : Integer
packageType : String
grossQuantity : Measure
netQuantity : Measure
stowagePosition : String
transportUnitId : String
details : CargoDetails
dg : DangerousGoodsSafetySheet
consignment : Consignment
dangerous : YesNoEnum
ConsignmentDetails
serialVersionUID : long
numberOfItems : Integer
ucr : String
placeWhenceConsigned : String
goodsReceiptPlace : String
carrier : Trader
consignor : Trader
consignee : Trader
notifyParty : Trader
paymentMethod : PaymentMethod
authorizationNumber : String
additionalInformation : String
DangerousGoodsSafetySheet
serialVersionUID : long
textualReference : String
dgClassification : String
unClass : String
unNumber : String
packingGroup : String
subsidiaryRisks : Set<String>
flashPoint : Double
marpolPollutionCode : String
emergencyInstruction : String
additionalInformation : String
cargoItem : CargoItem
BunkersRemainOnBoard
heavyFuelQuantity : Double
gasOilQuantity : Double
marineGasQuantity : Double
marineDieselOilQuantity : Double
otherOilQuantity : Double
deliveryReceipt : Boolean
MDHAttachment
serialVersionUID : long
databaseId : Long
number : String
gender : String
embarkationDate : Calendar
illness : String
symptomsDate : Calendar
reportedToPortMedical : boolean
state : String
caseDisposal : String
locationOfEvacuation : String
treatment : String
comments : String
crew : boolean
health : Health

Class	**AbstractMessage**

Class Diagram : port clearance request	
	An abstract class holds the common attributes of EPC messages; it represents ➢ the EPC Message Header attributes as ship Message Id, sender, sender duty, reporting System, sent time, reply URI and version; ➢ the Port Clearance information.
Class	**EPCRequestMessage** This class extends the aforementioned AbstractMessage class to represent the specific EPC Request for clearance notification; the message type is "FAL".
Class	**EPCCancelationMessage** This class extends the aforementioned AbstractMessage class to represent the specific EPC Cancelation notification. A cancellation message can be sent to the NSW to cancel a previously submitted request. A cancellation message that received a receipt will cease any further processing of the request and all previously received acknowledgement messages, if any, will be voided. The message type is "CANCEL".
Class	**EPCComment** This class extends the aforementioned AbstractMessage class to represent the specific EPC Comment Message; general comment to ship, port or authority to be read by human operator.
Class	**EPCReceipt** This class extends the aforementioned AbstractMessage class to represent the specific EPC Receipt Message synchronously transmitted on the aforementioned EPC messages arrival; a receipt stating that a message has been received and is being processed. This message, sent as an acknowledgement, does not contain any status of the request. The message type is "Receipt".
Class	**EPCAcknowledge** This class extends the aforementioned AbstractMessage class to represent the asynchronous response EPC Acknowledge Message; an acknowledgement that a message has been processed and that this message contains the status of the request. An acknowledgement message is sent to the ship when one or more authorities have processed a request and made a decision. Its message type is "ACK".

Class Diagram : port clearance request	
Class	**ShipCall** This class represents the PortClearance information of EPC messages; its attributes are journal number, arrival/departure flag, ship identification, port of call information, list of crew on board, list of passengers, health and waste information.
Class	**ShipIdentifier** This class represents the reported ship particulars as IMO, MMSI, call sign, ship name.
Class	**ShipParticulars** This class extends the aforementioned ShipIdentifier class to represent the additional attributes such as Inmarsat call number to ship, Gross tonnage, Net tonnage, ship type, the ship's operating company, security officer, certificate description.
Class	**PortCall** This class represents the port of call information. Its attributes are port of registration, voyage number, estimated time of arrival / departure at/from the port of call, actual time of arrival / departure at/from the port of call, the name of the organisation representing the ship (agent), the primary purpose of the call, the last / next port, the security level, last ten port calls.
Class	**Person** This class represents the person information; it includes the person’s name – family name, middle name, given name, the address and contact information.
Class	**PersonOnBoard** This class extends the aforementioned Person class to represent the person on board entity; its additional attributes are the date and place of birth, the nationality, visa number, embarkation port, visited ports.
Class	**Crew** This class extends the aforementioned PersonOnBoard class to represent the crew information; its attributes are reference, the duty, the master name, a list of possible dutiable or prohibited items.
Class	**CrewEffects** **Represents the CrewEffects data group.**
Class	**Passenger** This class extends the aforementioned PersonOnBoard class to represent the passenger information; its attributes are the

Class Diagram : port clearance request	
	port where the passenger disembarked, the transit flag.
Class	**Health** This class represents the health information.
Class	**MDHAttachment** This class represents the MeDical Health attachment.
Class	**Waste** It holds the waste information.
Class	**WasteDisposalInformation** It holds the waste disposal information.
Class	**Agent** This class represents the Agency.
Class	**CargoDeclartion** Represents the cargo declaration data group.
Class	**Consignment** Represents the consignment data group
Class	**AbstractCargoItem** Common fields of DangerousAndPollutingCargo and CargoItem.
Class	**CargoItem** Represents the items included in a consignment.
Class	**DangerousAndPollutingCargo** Represents the dangerous and polluting cargo items.
Class	**Security** Represents the the security data group.
Class	**WasteDeliveryReceipt** Represents the waste delivery report data group.
Class	**BunkersRemainOnBoard** Represents the bunkers on board group.
Class	**CivilLiabilityCertificatePollutingDamage** Represents the civil liability certificates for oil and bunker oil data groups.
Class	**ShipDefects** Represents the ship effects data group.

4.2.2 Resource Management

This module implements the NSW resource management. This module is used by the CRG and the Authority Information Exchange subsystems.

It includes the users' management as well as profiles and access rights management, and the reference data management including ships, shipping companies, countries, locations.

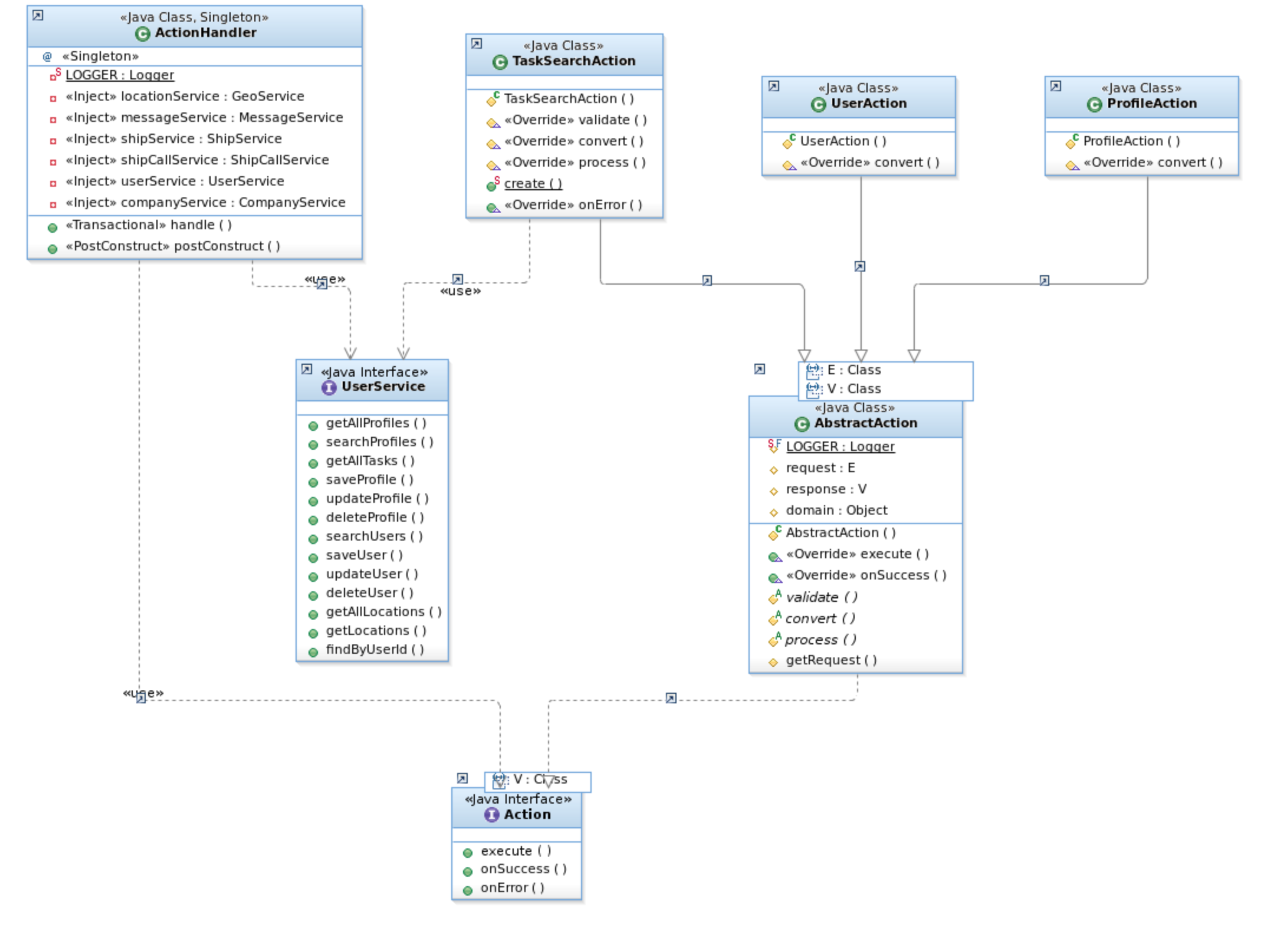
The implementation of all business services "respects" the Command Pattern. The benefit of this particular implementation is that the "*execute/process*" command is used for all the NSW entities as well as the *convert* – from DTO to domain and vice-versa – and *validate* commands. In addition, the *OnSuccess* and *OnError* handlers are commons.

4.2.2.1 UML Class Diagrams

4.2.2.2 Module: resource-management

4.2.2.2.1 Package: emsa.nsw.resources

Class Diagram : resource management services – user service

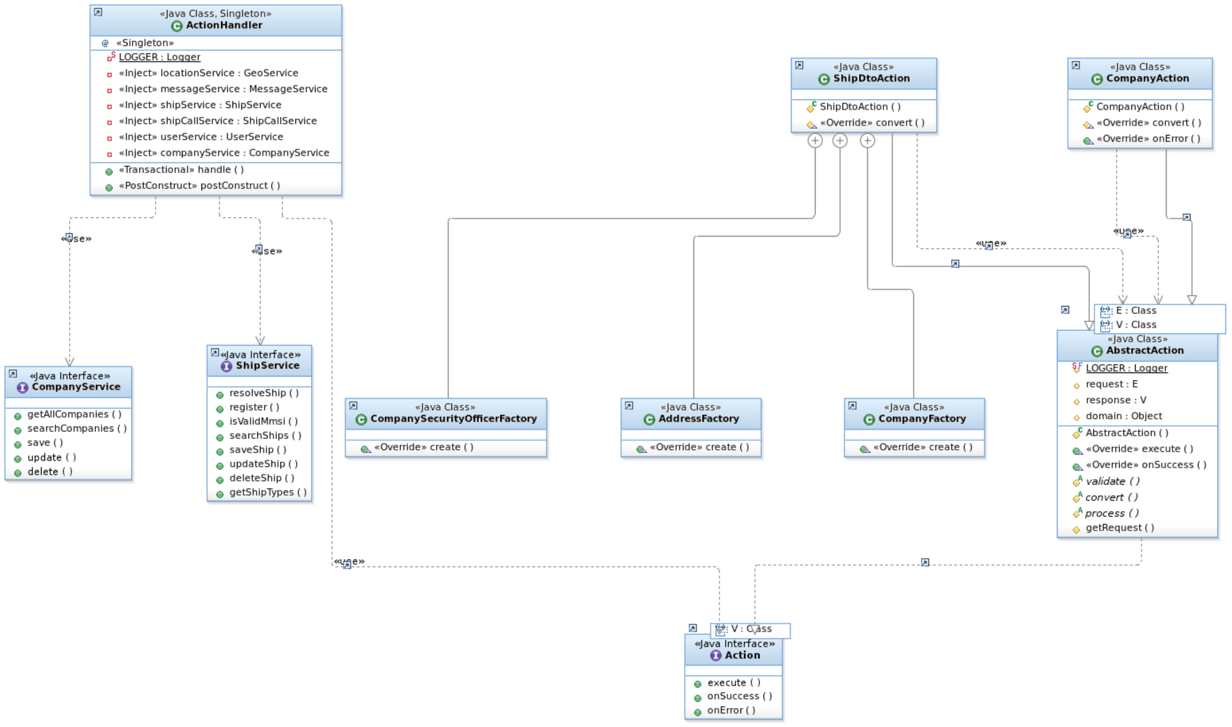


Interface	**Action** This common in interface represents the *Command Interface*. It defines the *execute* method as well as the handlers *OnSuccess* and *OnError*.
Class	**AbstractAction** This abstract class encapsulates data request. Furthermore, it defines some common operations that applied to all actions defined for the application. These common operations are: ➢ Conversion from the DTO object defined in spec to the corresponding domain object. ➢ Validation that includes data validation, reference data resolution and several business processes invocations. ➢ Process that performs the main business operation.

Class Diagram : resource management services – user service

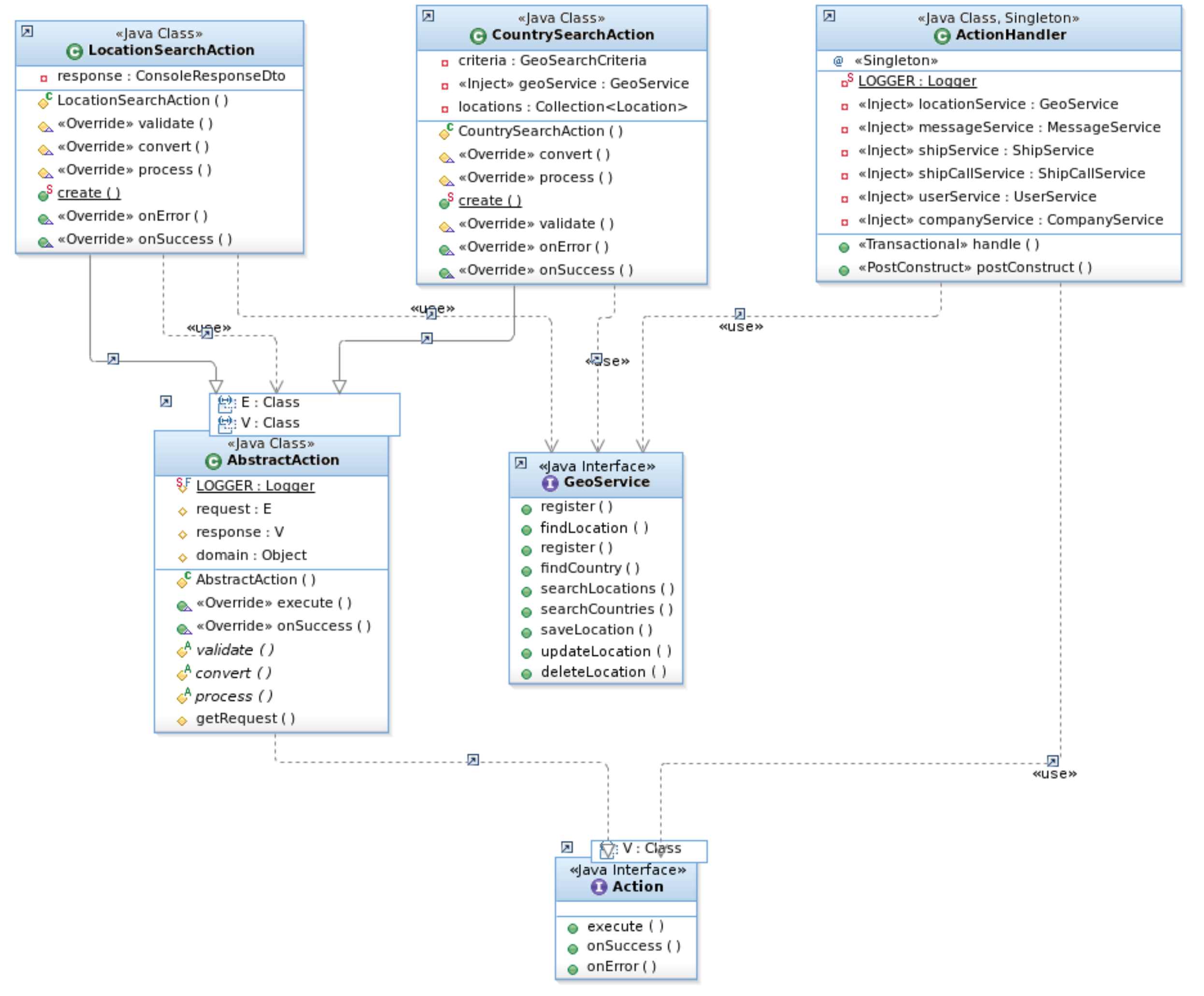
Class	**ActionHandler** This common class is a singleton that acts as the action invoker. It calls action's execute method and in case of failure calls the onError method, otherwise the onSucess method.
Interface	**UserService** This interface defines the methods for users and profiles management.
Class	**UserAction** This class implements (*ConcreteCommand*) the CRUD operations for user entity.
Class	**ProfileAction** This class implements (*ConcreteCommand*) the CRUD operations for profile entity.
Class	**TaskSearchAction** This class implements (*ConcreteCommand*) the profiles search functionality provided by web consoles (UI).

Class Diagram : resource management services – ship service



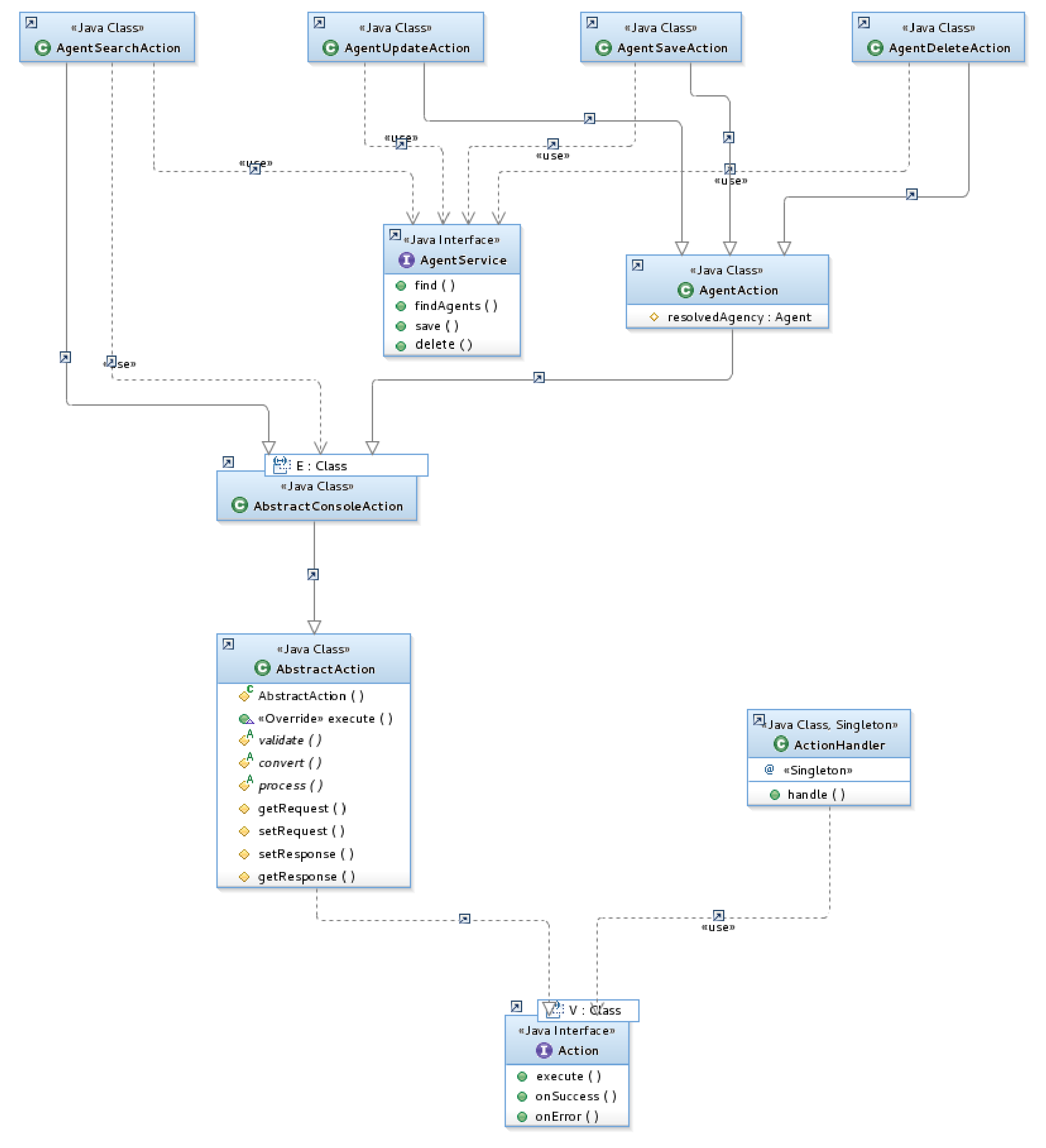
Class Diagram : resource management services – ship service	
Interface	**ShipService** This interface defines the methods for ships' management.
Class	**ShipDtoAction** This class implements (*ConcreteCommand*) the CRUD operations for ship entity.
Interface	**CompanyService** This interface defines the methods for shipping companies' management.
Class	**CompanyAction** This class implements (*ConcreteCommand*) the CRUD operations for shipping company entity.

Class Diagram : resource management services – geo service



Interface	**GeoService** This interface defines the methods for locations and countries management.
Class	**CountrySearchAction** This class implements (*ConcreteCommand*) the management of country entity.
Class	**LocationSearchAction** This class implements (*ConcreteCommand*) the management of location entity.

Class Diagram : resource management services – Agent service



Interface	**AgentService** This interface defines the methods for agencies management.
Class	**AgentSearchAction** Process for searching agencies.

Class Diagram : resource management services – Agent service	
Class	**AgentUpdateAction** Performs the steps for updating an Agency
Class	**AgentSaveAction** Performs the steps for saving an Agency
Class	**AgentDeleteAction** Performs the steps for deleting an Agency

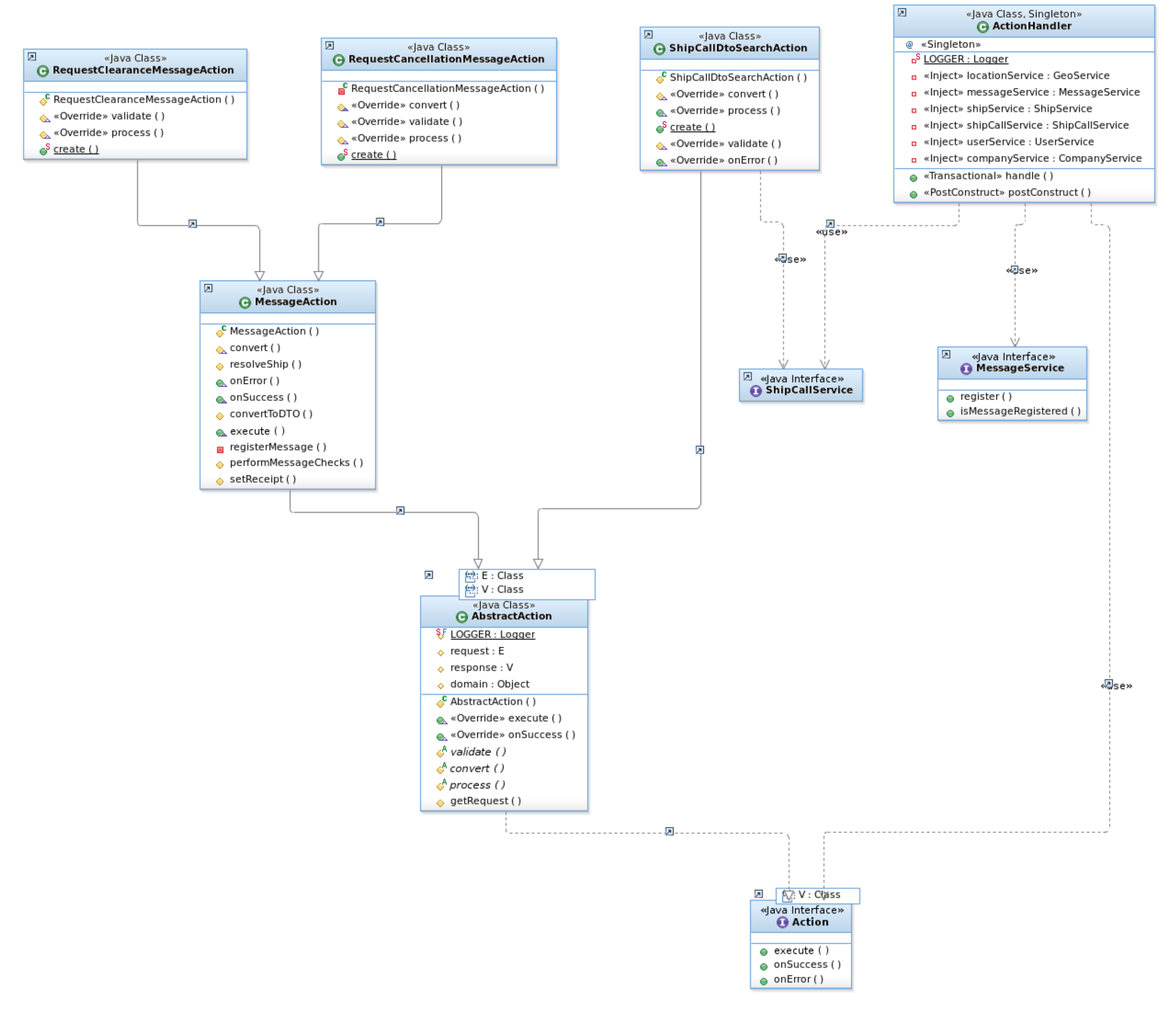
4.3 Common Reporting Gateway

The CRG subsystem provides an electronic interface between the ship or the ship representatives and authorities ashore. This communication is described by the NSWService in section 4.5 of this document.

The CRG subsystem also provides a Request/Response interface to receive ShipCall information from SSN system. This communication is described by SSN Message Services of the external EMSA SSN Central.

4.3.1 UML Class Diagrams

Class Diagram : common reporting gateway – port clearance & shipcall services



Interface	**MessageService** This interface defines the methods for Port Clearance management.
Class	**MessageAction** This abstract class encapsulates the processing of EPC messages.
Class	**RequestClearanceMessageAction** This class implements (*ConcreteCommand*) the processing of Port Clearance Request.
Class	**RequestCancelationMessageAction** This class implements (*ConcreteCommand*) the processing of Cancelation Message (of a previous request).

Class Diagram : common reporting gateway – port clearance & shipcall services	
Interface	**ShipCallService** This interface defines the methods for ShipCall information exchanged with SSN System.
Class	**ShipCallDtoSearchAction** This class implements the processing of ShipCall messages exchanged with SSN System.

4.4 Authority Information Exchange

The authority-information-exchange subsystem includes the components:

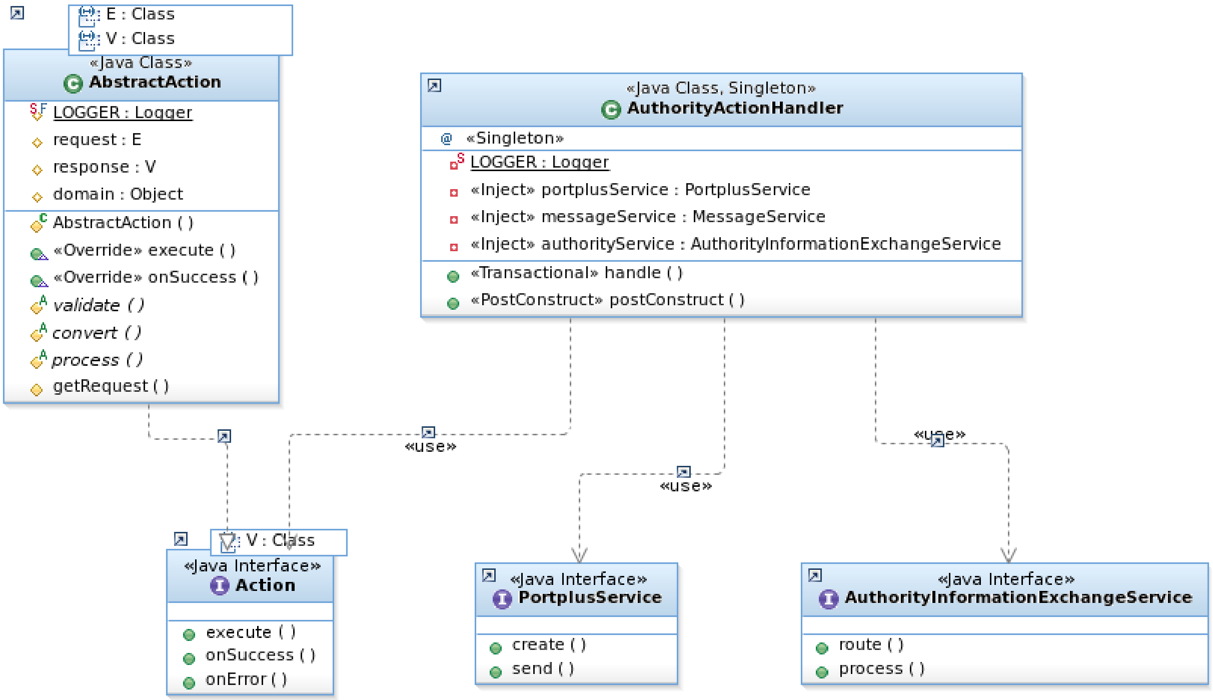
- Authority Information Exchange.
- PortPlus management.
- Resource management.
- Support module for tracing, logging.

The Authority subsystem provides an electronic interface between the aforementioned CRG system and authorities ashore. This communication is described by the NSWService in section 4.5 of this document.

The Authority subsystem also provides a PortPlus interface to submit PortPlus notifications to SSN system. This communication is described by SSN Message Services of the external EMSA SSN Central.

4.4.1 UML Class

Class Diagram : authority – information exchange & portplus services

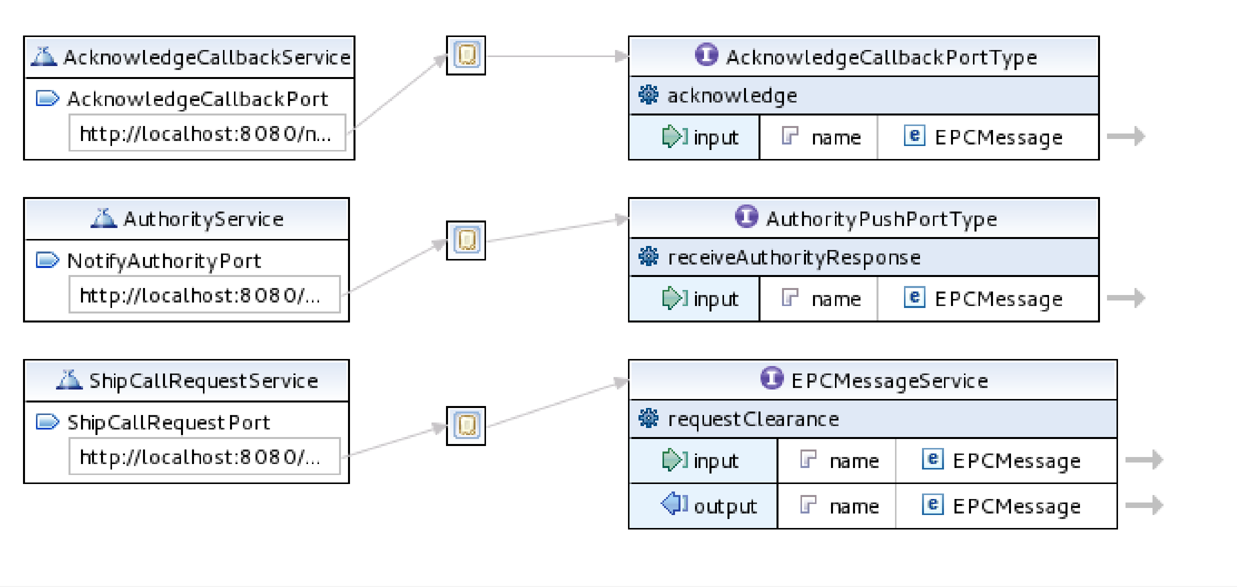


Class	**AuthorityActionHandler** This abstract class encapsulates the processing of port clearance messages.
Interface	**AuthorityInformationExchangeService** This interface defines the processing and routing of Port Clearance Request.
Interface	**PortplusService** This interface defines the creation and submission of Portplus notification to SSN system.

4.5 WebService: NSWService

The implementation of the NSW WebService shall define and manage the exchange of EPC messages between the ship or the ship representatives and authorities ashore.

Service Contract : nsw.wsdl



WSDL	**nsw.wsdl** Example of service contract WSDL file focused on EPC messages exchange; it is based on epc.xsd schema (data contract). It also defines the DataRequestorMessageService; i.e. the request callback to receive the asynchronous ShipCall responses from SSN system upon a ShipCall request (data contract of these messages is ssn.xsd).
Data contract	**epc.xsd**

Port Clearance (EPC) Messages

The EPC messages (SOAP over HTTP) exchanges between the ship or the ship representatives and authorities (Web Services) related to the NSW Domain as well as the relationship of these messages with the domain classes. More specifically,

- The **Port Clearance Request (EPCMessage** with type **FAL)** message is sent by a ship representative (acting as Ship Data Provider) to CRG system in order to **request** clearance to enter or leave the port. Message Information is represented by the EPCRequestMessage of the domain model.
- The **Port Clearance Receipt (EPCMessage** with type **Receipt)** message is synchronously sent by CRG system to the ship representative to inform that
  - its request is free of syntax errors and sufficiently complete to be forwarded to some or all authorities involved. The receipt message lists those authorities to which the request message had been forwarded; or
  - its request either contains syntax errors, or is incomplete, or contains information that cannot be processed by the CRG. This request will not be forwarded to the authorities and will not cause any further processing. Incomplete request messages

to a SW that do not allow for updates will be ignored. This request needs to be corrected and resent.

Message Information is represented by the EPCReceipt of the domain model.

The aforementioned **EPCMessage** exchange is provided by the *PortClearanceRequestService* implemented by CRG system.

The valid **Port Clearance Request** messages are forwarder to the corresponding Authority systems; this **notify** operation is provided by the *AuthorityService* and is implemented by Authority system. CRG acts as webservice client. Authority system synchronously responds with a receipt message.

CRG implements a **notifyCallback** operation to asynchronously receive the Authority corresponding response; the **notifyCallback** operation is provided by the *NotifyAuthorityCallbackService*. This operation triggers the creation of the **Acknowledgement** described below.

- The **Acknowledgement (EPCMessage** with type **ACK)** message is sent by CRG system to the ship provider when one or more authorities have processed a request and made a decision; thus, Ship Data Provider system should implement an *AcknowledgeCallbackService* to receive these messages. CRG acts as webservice client on this operation. Message Information is represented by the EPCAcknowledge of the domain model.

4.6 Automatic Partitions Creation

Responsibilities	Automatic creation of monthly partitions and associated tablespaces.
Stored procedure	IMP_SCHEMA.MNG_UTILS_PKG.ADD_PARTITIONS_PR
Action History	Every partition and tablespaces that is created is logged into the TLOG table. The outcome of the execution (failure/success) is logged into the database log tables (TLOG).
Processing logic	An Oracle job is scheduled to run periodically (at the last day of each calendar month) to execute the PL/SQL procedure that creates new partitions for all ShipCall related tables and associated tablespaces. • The location where the tablespace datafiles are to be created is defined under APPLICATION_PARAMETERS TBL_DATAFILE_PATH. • In case of failure, the procedure will send an email to a parameterizable set of email address(es) informing of the failure. • The manually execution of the PL/SQL procedure is possible by the database administrator using SQL plus or

	another IDE. The administrator may execute the following statement:
	BEGIN
	IMP_SCHEMA_DEV.MNG_UTILS_PKG.ADD_PARTITIONS_PR
	;
	  COMMIT;
	END;

Database Transactions	New partitions and tablespaces are created. The processing logic and errors are recorded into the TLOG table: TABLE TLOG, columns: ID NUMBER, LDATE DATE, LHSECS NUMBER, LLEVEL NUMBER, LSECTION VARCHAR2(2000), LTEXTE VARCHAR2(2000), LUSER VARCHAR2(30).

4.7 NSW-GI

The NSW-GI component implementation is based on source code extracted from SSN-GI's original codebase. As such, it provides a subset of the required functionalities already offered by SSN-GI, with appropriate modifications that allow its integration into the architectural and functional context of NSW. User authentication and authorisation in NSW-GI is performed in the same security context as the other NSW components.

The internal structure of the application is, for the most part, identical to that of SSN-GI, as presented in [R6], with the exception of the data-layer. The latter is modified in NSW-GI so that vessel position information is not retrieved directly from a database, but rather from the back-end of an actual operating instance of SSN-GI, via an appropriate HTTP, REST-service interface. Upon installation, each NSW-GI instance configuration binds it with a specific SSN user which has been associated with that particular MS. This user's visualisation permissions are used by SSN-GI in order to determine the subset of vessels for which position information is to be provided to the respective NSW-GI instance performing the request.

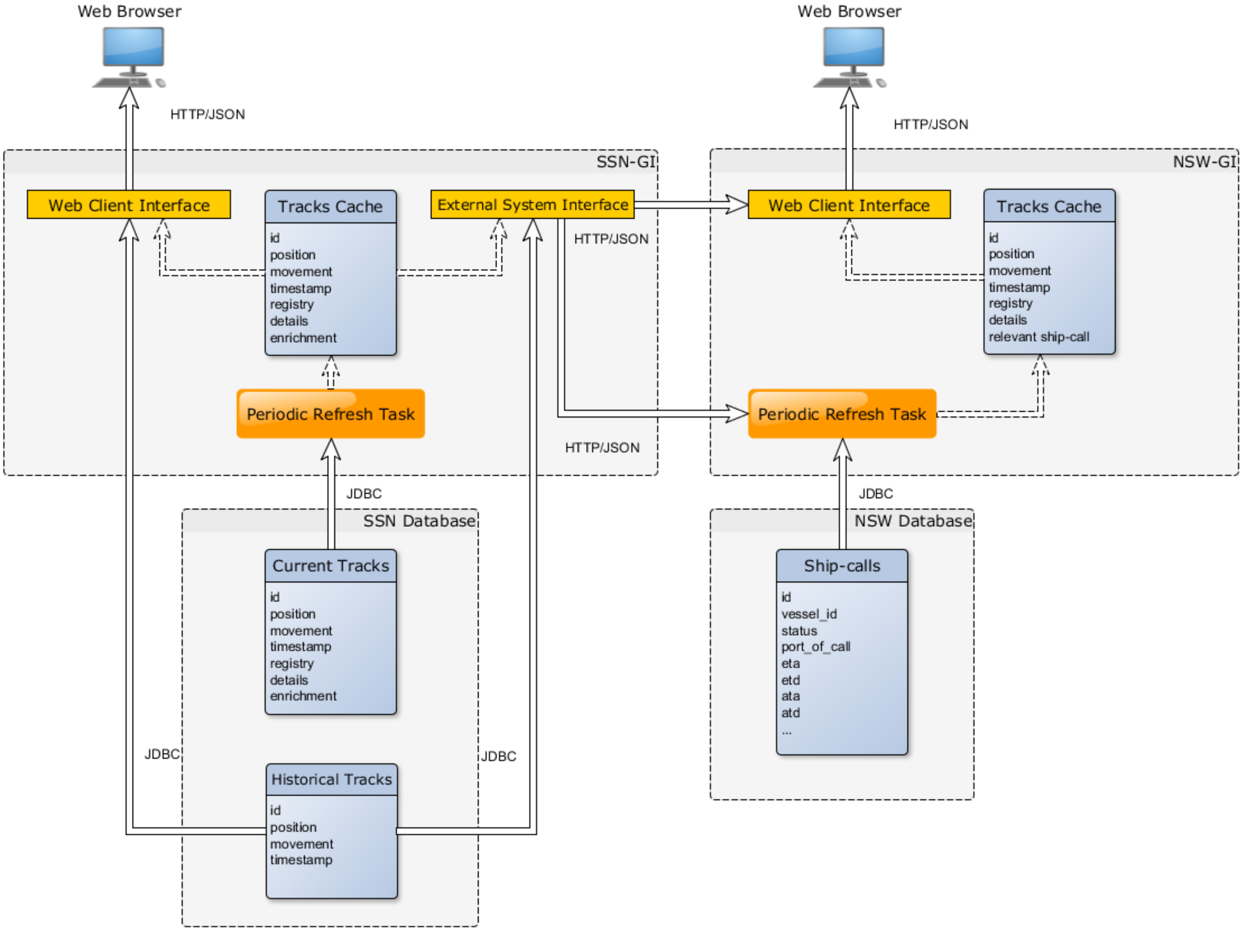


Figure 4-3 NSW-GI ship position data retrieval

Regarding the latest position information of vessels, NSW-GI maintains its own in-memory vessel tracks cache, similarly to SSN-GI, whose contents are refreshed periodically, every 3 minutes, via HTTP/JSON from the respective structure hosted in the latter's back-end. Once this information is retrieved from SSN-GI, it immediately becomes enriched using the latest ship-call information from the NSW database (table MOST_RELEVANT_SHIP_CALLS). Consequently, "live-track" requests originating from NSW-GI client web-browsers are handled asynchronously by the local cache, without affecting SSN-GI performance. However, historical-track requests made by NSW-GI clients are propagated directly to SSN-GI's backend, which in-turn retrieves the required information on demand from the SSN database.

It shall be noted that:

a) The tracks submitted by a VDM Data provider are visible by users with AIS_RECIPIENT role and visualization area included in the aforementioned "sender" provider areas;

b) MS terrestrial AIS define an SSN user with AIS_PROVIDER role and at least one provider area;

c) NSW Authority defines an SSN user with AIS_RECIPIENT role and visualization area the aforementioned provider area of the relevant MS terrestrial AIS.

5 Database Architectural Design

The data model supported by the NSW components: Common Reporting Gateway and Authority Information Exchange is identical. Both the components will maintain the data exchanged in a dedicated data store enabling them to be deployed and function separately. The database contains:

- Tables to store ship call related data – those reported in a clearance notification (via the XML/SOAP or the Web interfaces;
- EPC message exchange data; clearance request and acknowledgment processing status;
- The system resource management data for user accounts, ship registry, shipping database registry, locations registry, access rights etc.;
- Information related with the configuration of reporting formalities;
- The supported clearance model.

The database design consists of the physical data model. The Physical Data Model is depicted in a Table-Reference (TR) diagram that models the information system including the details of physical implementation.

5.1 Physical data Model

The physical design diagram of the database table objects is depicted in the following figures:

Figure 5-1: presents the tables that hold the ship calls and data relative to port calls, ship particulars, bunkers, civil liability certificates and the most relevant voyage per ship (to be used by NSW GI).

Figure 5-2: presents the tables that hold the ship call data relative to cargo and dangerous and polluting goods. Note: for consistency and completeness the table SHIP_CALLS is repeated as in previous figure.

Figure 5-3: presents the tables that hold the ship call data relative to ship's stores, security, as well as the EPC messages received, the acknowledgement messages sent and the clearance process status. Note: for consistency and completeness the table SHIP_CALLS is repeated as in previous figure.

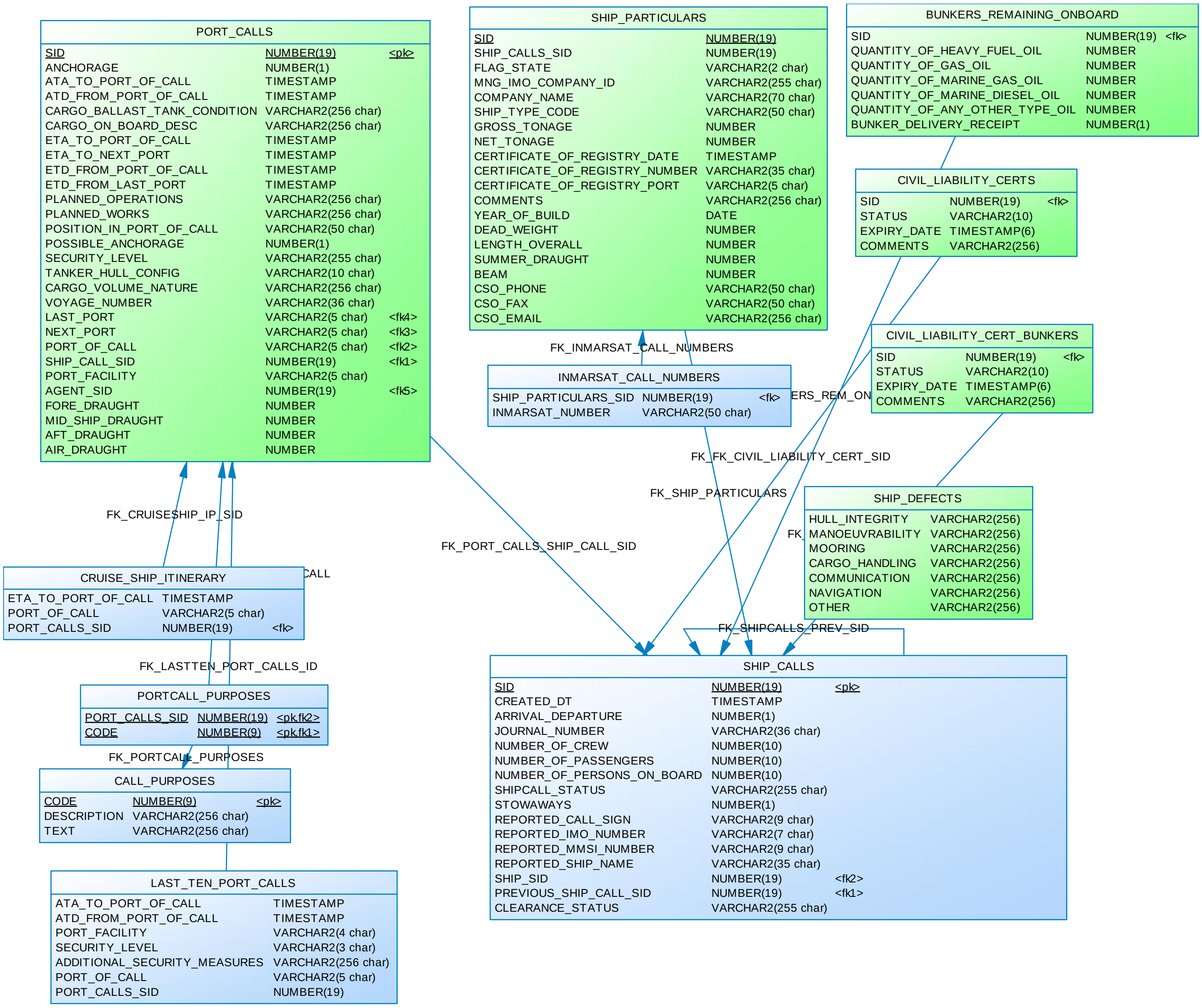
Figure 5-4: presents the tables that hold the attachments per ship call and group, ship call data relative to waste, waste receipt, crew and passenger lists. Note: for consistency and completeness the table SHIP_CALLS is repeated as in previous figure.

Figure 5-5: presents the ship, shipping companies and locations registries.

Figure 5-6: presents the user management, access rights management And the user session default parameters.

Figure 5-7: presents the regulatory information, application parameters, the SSN sevices configuration parameters and the NSW GI user, filter and Map configuration parameters tables.

Green colour indicates new or updated tables (based on the previous NSW database schema version).



PORT_CALLS

SID	NUMBER(19)	<pk>
ANCHORAGE	NUMBER(1)	
ATA_TO_PORT_OF_CALL	TIMESTAMP	
ATD_FROM_PORT_OF_CALL	TIMESTAMP	
CARGO_BALLAST_TANK_CONDITION	VARCHAR2(256 char)	
CARGO_ON_BOARD_DESC	VARCHAR2(256 char)	
ETA_TO_PORT_OF_CALL	TIMESTAMP	
ETA_TO_NEXT_PORT	TIMESTAMP	
ETD_FROM_PORT_OF_CALL	TIMESTAMP	
ETD_FROM_LAST_PORT	TIMESTAMP	
PLANNED_OPERATIONS	VARCHAR2(256 char)	
PLANNED_WORKS	VARCHAR2(256 char)	
POSITION_IN_PORT_OF_CALL	VARCHAR2(50 char)	
POSSIBLE_ANCHORAGE	NUMBER(1)	
SECURITY_LEVEL	VARCHAR2(255 char)	
TANKER_HULL_CONFIG	VARCHAR2(10 char)	
CARGO_VOLUME_NATURE	VARCHAR2(256 char)	
VOYAGE_NUMBER	VARCHAR2(36 char)	
LAST_PORT	VARCHAR2(5 char)	<fk4>
NEXT_PORT	VARCHAR2(5 char)	<fk3>
PORT_OF_CALL	VARCHAR2(5 char)	<fk2>
SHIP_CALL_SID	NUMBER(19)	<fk1>
PORT_FACILITY	VARCHAR2(5 char)	
AGENT_SID	NUMBER(19)	<fk5>
FORE_DRAUGHT	NUMBER	
MID_SHIP_DRAUGHT	NUMBER	
AFT_DRAUGHT	NUMBER	
AIR_DRAUGHT	NUMBER	

SHIP_PARTICULARS

SID	NUMBER(19)
SHIP_CALLS_SID	NUMBER(19)
FLAG_STATE	VARCHAR2(2 char)
MNG_IMO_COMPANY_ID	VARCHAR2(255 char)
COMPANY_NAME	VARCHAR2(70 char)
SHIP_TYPE_CODE	VARCHAR2(50 char)
GROSS_TONAGE	NUMBER
NET_TONAGE	NUMBER
CERTIFICATE_OF_REGISTRY_DATE	TIMESTAMP
CERTIFICATE_OF_REGISTRY_NUMBER	VARCHAR2(35 char)
CERTIFICATE_OF_REGISTRY_PORT	VARCHAR2(5 char)
COMMENTS	VARCHAR2(256 char)
YEAR_OF_BUILD	DATE
DEAD_WEIGHT	NUMBER
LENGTH_OVERALL	NUMBER
SUMMER_DRAUGHT	NUMBER
BEAM	NUMBER
CSO_PHONE	VARCHAR2(50 char)
CSO_FAX	VARCHAR2(50 char)
CSO_EMAIL	VARCHAR2(256 char)

BUNKERS_REMAINING_ONBOARD

SID	NUMBER(19)	<fk>
QUANTITY_OF_HEAVY_FUEL_OIL	NUMBER	
QUANTITY_OF_GAS_OIL	NUMBER	
QUANTITY_OF_MARINE_GAS_OIL	NUMBER	
QUANTITY_OF_MARINE_DIESEL_OIL	NUMBER	
QUANTITY_OF_ANY_OTHER_TYPE_OIL	NUMBER	
BUNKER_DELIVERY_RECEIPT	NUMBER(1)	

CIVIL_LIABILITY_CERTS

SID	NUMBER(19)	<fk>
STATUS	VARCHAR2(10)	
EXPIRY_DATE	TIMESTAMP(6)	
COMMENTS	VARCHAR2(256)	

CIVIL_LIABILITY_CERT_BUNKERS

SID	NUMBER(19)	<fk>
STATUS	VARCHAR2(10)	
EXPIRY_DATE	TIMESTAMP(6)	
COMMENTS	VARCHAR2(256)	

INMARSAT_CALL_NUMBERS

SHIP_PARTICULARS_SID	NUMBER(19)	<fk>
INMARSAT_NUMBER	VARCHAR2(50 char)	

SHIP_DEFECTS

HULL_INTEGRITY	VARCHAR2(256)
MANOEUVRABILITY	VARCHAR2(256)
MOORING	VARCHAR2(256)
CARGO_HANDLING	VARCHAR2(256)
COMMUNICATION	VARCHAR2(256)
NAVIGATION	VARCHAR2(256)
OTHER	VARCHAR2(256)

CRUISE_SHIP_ITINERARY

ETA_TO_PORT_OF_CALL	TIMESTAMP	
PORT_OF_CALL	VARCHAR2(5 char)	
PORT_CALLS_SID	NUMBER(19)	<fk>

PORTCALL_PURPOSES

PORT_CALLS_SID	NUMBER(19)	<pk,fk2>
CODE	NUMBER(9)	<pk,fk1>

CALL_PURPOSES

CODE	NUMBER(9)	<pk>
DESCRIPTION	VARCHAR2(256 char)	
TEXT	VARCHAR2(256 char)	

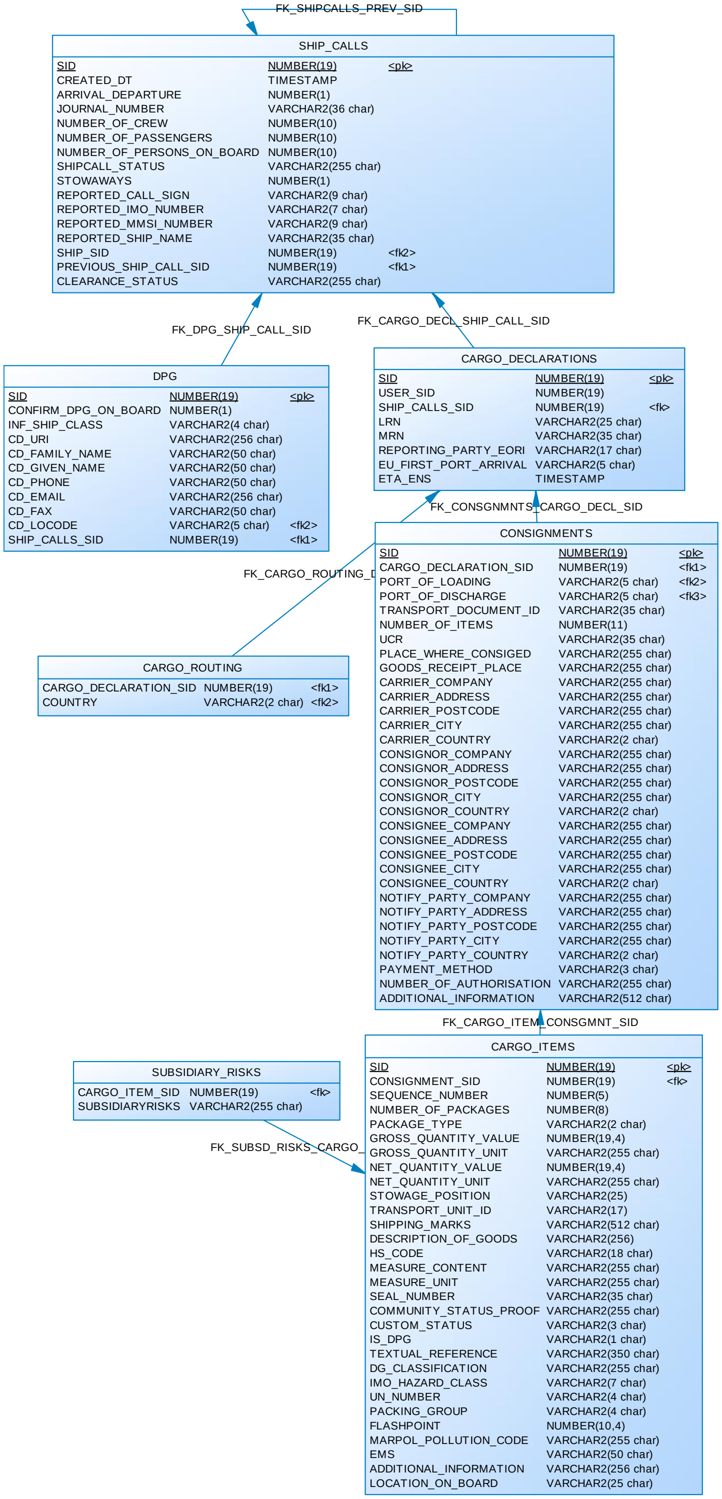
SHIP_CALLS

SID	NUMBER(19)	<pk>
CREATED_DT	TIMESTAMP	
ARRIVAL_DEPARTURE	NUMBER(1)	
JOURNAL_NUMBER	VARCHAR2(36 char)	
NUMBER_OF_CREW	NUMBER(10)	
NUMBER_OF_PASSENGERS	NUMBER(10)	
NUMBER_OF_PERSONS_ON_BOARD	NUMBER(10)	
SHIPCALL_STATUS	VARCHAR2(255 char)	
STOWAWAYS	NUMBER(1)	
REPORTED_CALL_SIGN	VARCHAR2(9 char)	
REPORTED_IMO_NUMBER	VARCHAR2(7 char)	
REPORTED_MMSI_NUMBER	VARCHAR2(9 char)	
REPORTED_SHIP_NAME	VARCHAR2(35 char)	
SHIP_SID	NUMBER(19)	<fk2>
PREVIOUS_SHIP_CALL_SID	NUMBER(19)	<fk1>
CLEARANCE_STATUS	VARCHAR2(255 char)	

LAST_TEN_PORT_CALLS

ATA_TO_PORT_OF_CALL	TIMESTAMP
ATD_FROM_PORT_OF_CALL	TIMESTAMP
PORT_FACILITY	VARCHAR2(4 char)
SECURITY_LEVEL	VARCHAR2(3 char)
ADDITIONAL_SECURITY_MEASURES	VARCHAR2(256 char)
PORT_OF_CALL	VARCHAR2(5 char)
PORT_CALLS_SID	NUMBER(19)

Figure 5-1 Ship Calls 1 - Physical Design Diagram


FK_SHIPCALLS_PREV_SID
FK_DPG_SHIP_CALL_SID
FK_CARGO_DECL_SHIP_CALL_SID
FK_CONSGNMNTS_CARGO_DECL_SID
FK_CARGO_ROUTING_D
FK_CARGO_ITEM_CONSGMNT_SID
FK_SUBSD_RISKS_CARGO_

SHIP_CALLS

SID	NUMBER(19)	<pk>
CREATED_DT	TIMESTAMP	
ARRIVAL_DEPARTURE	NUMBER(1)	
JOURNAL_NUMBER	VARCHAR2(36 char)	
NUMBER_OF_CREW	NUMBER(10)	
NUMBER_OF_PASSENGERS	NUMBER(10)	
NUMBER_OF_PERSONS_ON_BOARD	NUMBER(10)	
SHIPCALL_STATUS	VARCHAR2(255 char)	
STOWAWAYS	NUMBER(1)	
REPORTED_CALL_SIGN	VARCHAR2(9 char)	
REPORTED_IMO_NUMBER	VARCHAR2(7 char)	
REPORTED_MMSI_NUMBER	VARCHAR2(9 char)	
REPORTED_SHIP_NAME	VARCHAR2(35 char)	
SHIP_SID	NUMBER(19)	<fk2>
PREVIOUS_SHIP_CALL_SID	NUMBER(19)	<fk1>
CLEARANCE_STATUS	VARCHAR2(255 char)	

DPG

SID	NUMBER(19)	<pk>
CONFIRM_DPG_ON_BOARD	NUMBER(1)	
INF_SHIP_CLASS	VARCHAR2(4 char)	
CD_URI	VARCHAR2(256 char)	
CD_FAMILY_NAME	VARCHAR2(50 char)	
CD_GIVEN_NAME	VARCHAR2(50 char)	
CD_PHONE	VARCHAR2(50 char)	
CD_EMAIL	VARCHAR2(256 char)	
CD_FAX	VARCHAR2(50 char)	
CD_LOCODE	VARCHAR2(5 char)	<fk2>
SHIP_CALLS_SID	NUMBER(19)	<fk1>

CARGO_DECLARATIONS

SID	NUMBER(19)	<pk>
USER_SID	NUMBER(19)	
SHIP_CALLS_SID	NUMBER(19)	<fk>
LRN	VARCHAR2(25 char)	
MRN	VARCHAR2(35 char)	
REPORTING_PARTY_EORI	VARCHAR2(17 char)	
EU_FIRST_PORT_ARRIVAL	VARCHAR2(5 char)	
ETA_ENS	TIMESTAMP	

CONSIGNMENTS

SID	NUMBER(19)	<pk>
CARGO_DECLARATION_SID	NUMBER(19)	<fk1>
PORT_OF_LOADING	VARCHAR2(5 char)	<fk2>
PORT_OF_DISCHARGE	VARCHAR2(5 char)	<fk3>
TRANSPORT_DOCUMENT_ID	VARCHAR2(35 char)	
NUMBER_OF_ITEMS	NUMBER(11)	
UCR	VARCHAR2(35 char)	
PLACE_WHERE_CONSIGED	VARCHAR2(255 char)	
GOODS_RECEIPT_PLACE	VARCHAR2(255 char)	
CARRIER_COMPANY	VARCHAR2(255 char)	
CARRIER_ADDRESS	VARCHAR2(255 char)	
CARRIER_POSTCODE	VARCHAR2(255 char)	
CARRIER_CITY	VARCHAR2(255 char)	
CARRIER_COUNTRY	VARCHAR2(2 char)	
CONSIGNOR_COMPANY	VARCHAR2(255 char)	
CONSIGNOR_ADDRESS	VARCHAR2(255 char)	
CONSIGNOR_POSTCODE	VARCHAR2(255 char)	
CONSIGNOR_CITY	VARCHAR2(255 char)	
CONSIGNOR_COUNTRY	VARCHAR2(2 char)	
CONSIGNEE_COMPANY	VARCHAR2(255 char)	
CONSIGNEE_ADDRESS	VARCHAR2(255 char)	
CONSIGNEE_POSTCODE	VARCHAR2(255 char)	
CONSIGNEE_CITY	VARCHAR2(255 char)	
CONSIGNEE_COUNTRY	VARCHAR2(2 char)	
NOTIFY_PARTY_COMPANY	VARCHAR2(255 char)	
NOTIFY_PARTY_ADDRESS	VARCHAR2(255 char)	
NOTIFY_PARTY_POSTCODE	VARCHAR2(255 char)	
NOTIFY_PARTY_CITY	VARCHAR2(255 char)	
NOTIFY_PARTY_COUNTRY	VARCHAR2(2 char)	
PAYMENT_METHOD	VARCHAR2(3 char)	
NUMBER_OF_AUTHORISATION	VARCHAR2(255 char)	
ADDITIONAL_INFORMATION	VARCHAR2(512 char)	

CARGO_ROUTING

CARGO_DECLARATION_SID	NUMBER(19)	<fk1>
COUNTRY	VARCHAR2(2 char)	<fk2>

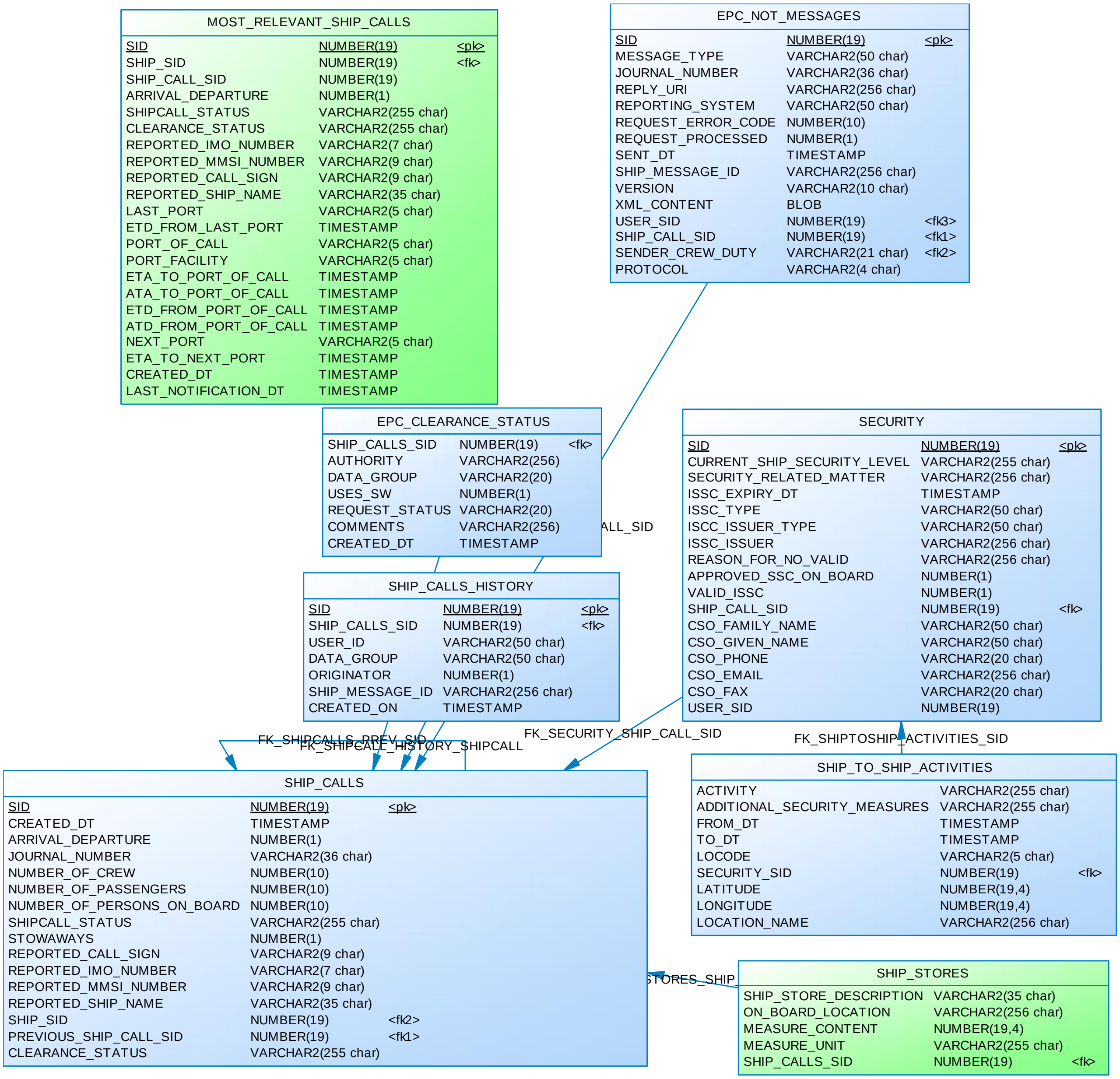
SUBSIDIARY_RISKS

CARGO_ITEM_SID	NUMBER(19)	<fk>
SUBSIDIARYRISKS	VARCHAR2(255 char)	

CARGO_ITEMS

SID	NUMBER(19)	<pk>
CONSIGNMENT_SID	NUMBER(19)	<fk>
SEQUENCE_NUMBER	NUMBER(5)	
NUMBER_OF_PACKAGES	NUMBER(8)	
PACKAGE_TYPE	VARCHAR2(2 char)	
GROSS_QUANTITY_VALUE	NUMBER(19,4)	
GROSS_QUANTITY_UNIT	VARCHAR2(255 char)	
NET_QUANTITY_VALUE	NUMBER(19,4)	
NET_QUANTITY_UNIT	VARCHAR2(255 char)	
STOWAGE_POSITION	VARCHAR2(25)	
TRANSPORT_UNIT_ID	VARCHAR2(17)	
SHIPPING_MARKS	VARCHAR2(512 char)	
DESCRIPTION_OF_GOODS	VARCHAR2(256)	
HS_CODE	VARCHAR2(18 char)	
MEASURE_CONTENT	VARCHAR2(255 char)	
MEASURE_UNIT	VARCHAR2(255 char)	
SEAL_NUMBER	VARCHAR2(35 char)	
COMMUNITY_STATUS_PROOF	VARCHAR2(255 char)	
CUSTOM_STATUS	VARCHAR2(3 char)	
IS_DPG	VARCHAR2(1 char)	
TEXTUAL_REFERENCE	VARCHAR2(350 char)	
DG_CLASSIFICATION	VARCHAR2(255 char)	
IMO_HAZARD_CLASS	VARCHAR2(7 char)	
UN_NUMBER	VARCHAR2(4 char)	
PACKING_GROUP	VARCHAR2(4 char)	
FLASHPOINT	NUMBER(10,4)	
MARPOL_POLLUTION_CODE	VARCHAR2(255 char)	
EMS	VARCHAR2(50 char)	
ADDITIONAL_INFORMATION	VARCHAR2(256 char)	
LOCATION_ON_BOARD	VARCHAR2(25 char)	

Figure 5-2 Ship Calls 2 - Physical Design Diagram



MOST_RELEVANT_SHIP_CALLS		
SID	NUMBER(19)	<pk>
SHIP_SID	NUMBER(19)	<fk>
SHIP_CALL_SID	NUMBER(19)	
ARRIVAL_DEPARTURE	NUMBER(1)	
SHIPCALL_STATUS	VARCHAR2(255 char)	
CLEARANCE_STATUS	VARCHAR2(255 char)	
REPORTED_IMO_NUMBER	VARCHAR2(7 char)	
REPORTED_MMSI_NUMBER	VARCHAR2(9 char)	
REPORTED_CALL_SIGN	VARCHAR2(9 char)	
REPORTED_SHIP_NAME	VARCHAR2(35 char)	
LAST_PORT	VARCHAR2(5 char)	
ETD_FROM_LAST_PORT	TIMESTAMP	
PORT_OF_CALL	VARCHAR2(5 char)	
PORT_FACILITY	VARCHAR2(5 char)	
ETA_TO_PORT_OF_CALL	TIMESTAMP	
ATA_TO_PORT_OF_CALL	TIMESTAMP	
ETD_FROM_PORT_OF_CALL	TIMESTAMP	
ATD_FROM_PORT_OF_CALL	TIMESTAMP	
NEXT_PORT	VARCHAR2(5 char)	
ETA_TO_NEXT_PORT	TIMESTAMP	
CREATED_DT	TIMESTAMP	
LAST_NOTIFICATION_DT	TIMESTAMP	

EPC_NOT_MESSAGES		
SID	NUMBER(19)	<pk>
MESSAGE_TYPE	VARCHAR2(50 char)	
JOURNAL_NUMBER	VARCHAR2(36 char)	
REPLY_URI	VARCHAR2(256 char)	
REPORTING_SYSTEM	VARCHAR2(50 char)	
REQUEST_ERROR_CODE	NUMBER(10)	
REQUEST_PROCESSED	NUMBER(1)	
SENT_DT	TIMESTAMP	
SHIP_MESSAGE_ID	VARCHAR2(256 char)	
VERSION	VARCHAR2(10 char)	
XML_CONTENT	BLOB	
USER_SID	NUMBER(19)	<fk3>
SHIP_CALL_SID	NUMBER(19)	<fk1>
SENDER_CREW_DUTY	VARCHAR2(21 char)	<fk2>
PROTOCOL	VARCHAR2(4 char)	

EPC_CLEARANCE_STATUS		
SHIP_CALLS_SID	NUMBER(19)	<fk>
AUTHORITY	VARCHAR2(256)	
DATA_GROUP	VARCHAR2(20)	
USES_SW	NUMBER(1)	
REQUEST_STATUS	VARCHAR2(20)	
COMMENTS	VARCHAR2(256)	
CREATED_DT	TIMESTAMP	

SECURITY		
SID	NUMBER(19)	<pk>
CURRENT_SHIP_SECURITY_LEVEL	VARCHAR2(255 char)	
SECURITY_RELATED_MATTER	VARCHAR2(256 char)	
ISSC_EXPIRY_DT	TIMESTAMP	
ISSC_TYPE	VARCHAR2(50 char)	
ISCC_ISSUER_TYPE	VARCHAR2(50 char)	
ISSC_ISSUER	VARCHAR2(256 char)	
REASON_FOR_NO_VALID	VARCHAR2(256 char)	
APPROVED_SSC_ON_BOARD	NUMBER(1)	
VALID_ISSC	NUMBER(1)	
SHIP_CALL_SID	NUMBER(19)	<fk>
CSO_FAMILY_NAME	VARCHAR2(50 char)	
CSO_GIVEN_NAME	VARCHAR2(50 char)	
CSO_PHONE	VARCHAR2(20 char)	
CSO_EMAIL	VARCHAR2(256 char)	
CSO_FAX	VARCHAR2(20 char)	
USER_SID	NUMBER(19)	

SHIP_CALLS_HISTORY		
SID	NUMBER(19)	<pk>
SHIP_CALLS_SID	NUMBER(19)	<fk>
USER_ID	VARCHAR2(50 char)	
DATA_GROUP	VARCHAR2(50 char)	
ORIGINATOR	NUMBER(1)	
SHIP_MESSAGE_ID	VARCHAR2(256 char)	
CREATED_ON	TIMESTAMP	

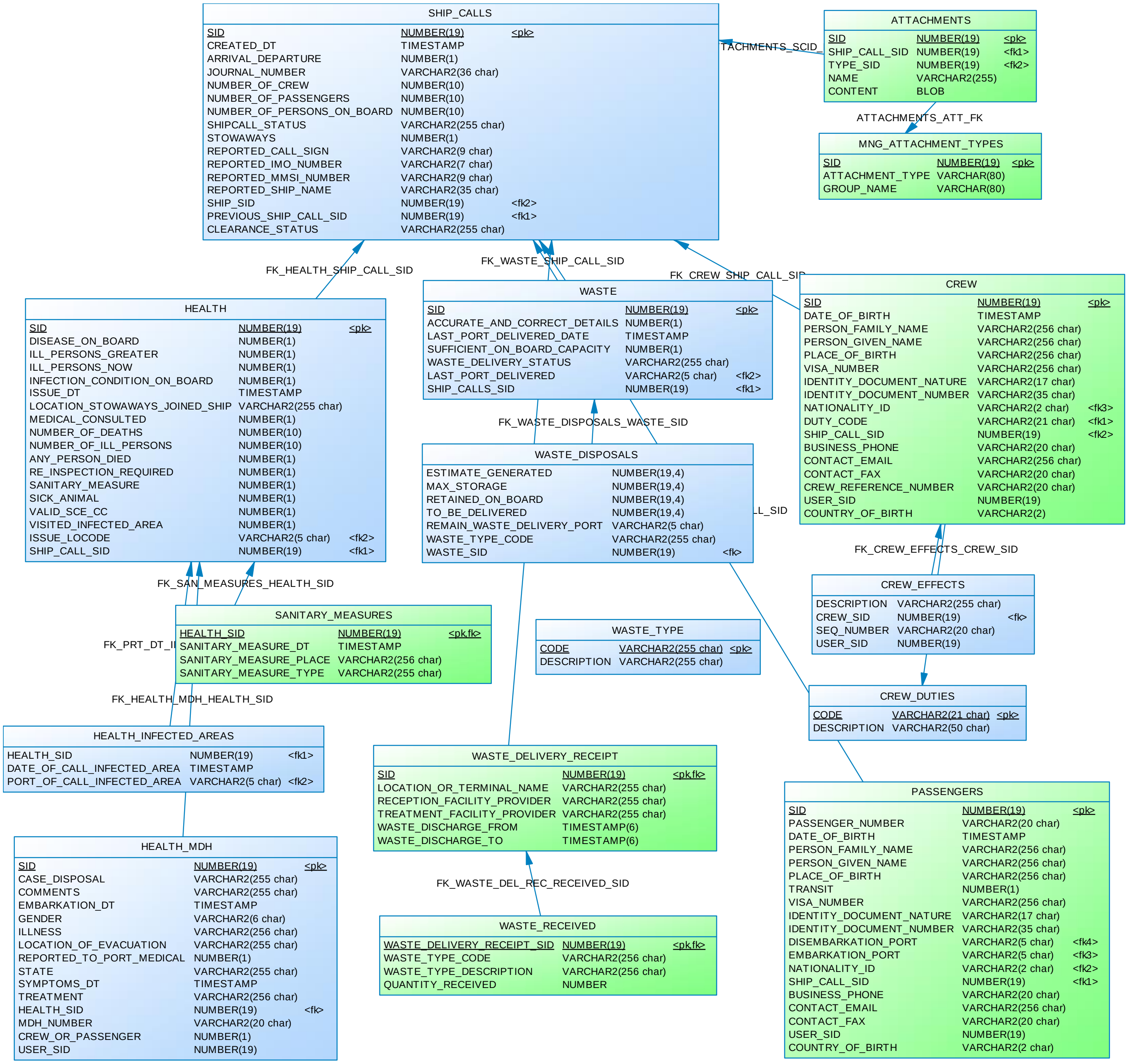
SHIP_CALLS		
SID	NUMBER(19)	<pk>
CREATED_DT	TIMESTAMP	
ARRIVAL_DEPARTURE	NUMBER(1)	
JOURNAL_NUMBER	VARCHAR2(36 char)	
NUMBER_OF_CREW	NUMBER(10)	
NUMBER_OF_PASSENGERS	NUMBER(10)	
NUMBER_OF_PERSONS_ON_BOARD	NUMBER(10)	
SHIPCALL_STATUS	VARCHAR2(255 char)	
STOWAWAYS	NUMBER(1)	
REPORTED_CALL_SIGN	VARCHAR2(9 char)	
REPORTED_IMO_NUMBER	VARCHAR2(7 char)	
REPORTED_MMSI_NUMBER	VARCHAR2(9 char)	
REPORTED_SHIP_NAME	VARCHAR2(35 char)	
SHIP_SID	NUMBER(19)	<fk2>
PREVIOUS_SHIP_CALL_SID	NUMBER(19)	<fk1>
CLEARANCE_STATUS	VARCHAR2(255 char)	

SHIP_TO_SHIP_ACTIVITIES		
ACTIVITY	VARCHAR2(255 char)	
ADDITIONAL_SECURITY_MEASURES	VARCHAR2(255 char)	
FROM_DT	TIMESTAMP	
TO_DT	TIMESTAMP	
LOCODE	VARCHAR2(5 char)	
SECURITY_SID	NUMBER(19)	<fk>
LATITUDE	NUMBER(19,4)	
LONGITUDE	NUMBER(19,4)	
LOCATION_NAME	VARCHAR2(256 char)	

SHIP_STORES		
SHIP_STORE_DESCRIPTION	VARCHAR2(35 char)	
ON_BOARD_LOCATION	VARCHAR2(256 char)	
MEASURE_CONTENT	NUMBER(19,4)	
MEASURE_UNIT	VARCHAR2(255 char)	
SHIP_CALLS_SID	NUMBER(19)	<fk>

ALL_SID
FK_SHIPCALLS_PREV_SID
FK_SHIPCALL_HISTORY_SHIPCALL
FK_SECURITY_SHIP_CALL_SID
FK_SHIPTOSHIP_ACTIVITIES_SID
STORES_SHIP

Figure 5-3 Ship Calls 3 - Physical Design Diagram



SHIP_CALLS

SID	NUMBER(19)	<pk>
CREATED_DT	TIMESTAMP	
ARRIVAL_DEPARTURE	NUMBER(1)	
JOURNAL_NUMBER	VARCHAR2(36 char)	
NUMBER_OF_CREW	NUMBER(10)	
NUMBER_OF_PASSENGERS	NUMBER(10)	
NUMBER_OF_PERSONS_ON_BOARD	NUMBER(10)	
SHIPCALL_STATUS	VARCHAR2(255 char)	
STOWAWAYS	NUMBER(1)	
REPORTED_CALL_SIGN	VARCHAR2(9 char)	
REPORTED_IMO_NUMBER	VARCHAR2(7 char)	
REPORTED_MMSI_NUMBER	VARCHAR2(9 char)	
REPORTED_SHIP_NAME	VARCHAR2(35 char)	
SHIP_SID	NUMBER(19)	<fk2>
PREVIOUS_SHIP_CALL_SID	NUMBER(19)	<fk1>
CLEARANCE_STATUS	VARCHAR2(255 char)	

ATTACHMENTS

SID	NUMBER(19)	<pk>
SHIP_CALL_SID	NUMBER(19)	<fk1>
TYPE_SID	NUMBER(19)	<fk2>
NAME	VARCHAR2(255)	
CONTENT	BLOB	

MNG_ATTACHMENT_TYPES

SID	NUMBER(19)	<pk>
ATTACHMENT_TYPE	VARCHAR(80)	
GROUP_NAME	VARCHAR(80)	

HEALTH

SID	NUMBER(19)	<pk>
DISEASE_ON_BOARD	NUMBER(1)	
ILL_PERSONS_GREATER	NUMBER(1)	
ILL_PERSONS_NOW	NUMBER(1)	
INFECTION_CONDITION_ON_BOARD	NUMBER(1)	
ISSUE_DT	TIMESTAMP	
LOCATION_STOWAWAYS_JOINED_SHIP	VARCHAR2(255 char)	
MEDICAL_CONSULTED	NUMBER(1)	
NUMBER_OF_DEATHS	NUMBER(10)	
NUMBER_OF_ILL_PERSONS	NUMBER(10)	
ANY_PERSON_DIED	NUMBER(1)	
RE_INSPECTION_REQUIRED	NUMBER(1)	
SANITARY_MEASURE	NUMBER(1)	
SICK_ANIMAL	NUMBER(1)	
VALID_SCE_CC	NUMBER(1)	
VISITED_INFECTED_AREA	NUMBER(1)	
ISSUE_LOCODE	VARCHAR2(5 char)	<fk2>
SHIP_CALL_SID	NUMBER(19)	<fk1>

WASTE

SID	NUMBER(19)	<pk>
ACCURATE_AND_CORRECT_DETAILS	NUMBER(1)	
LAST_PORT_DELIVERED_DATE	TIMESTAMP	
SUFFICIENT_ON_BOARD_CAPACITY	NUMBER(1)	
WASTE_DELIVERY_STATUS	VARCHAR2(255 char)	
LAST_PORT_DELIVERED	VARCHAR2(5 char)	<fk2>
SHIP_CALLS_SID	NUMBER(19)	<fk1>

CREW

SID	NUMBER(19)	<pk>
DATE_OF_BIRTH	TIMESTAMP	
PERSON_FAMILY_NAME	VARCHAR2(256 char)	
PERSON_GIVEN_NAME	VARCHAR2(256 char)	
PLACE_OF_BIRTH	VARCHAR2(256 char)	
VISA_NUMBER	VARCHAR2(256 char)	
IDENTITY_DOCUMENT_NATURE	VARCHAR2(17 char)	
IDENTITY_DOCUMENT_NUMBER	VARCHAR2(35 char)	
NATIONALITY_ID	VARCHAR2(2 char)	<fk3>
DUTY_CODE	VARCHAR2(21 char)	<fk1>
SHIP_CALL_SID	NUMBER(19)	<fk2>
BUSINESS_PHONE	VARCHAR2(20 char)	
CONTACT_EMAIL	VARCHAR2(256 char)	
CONTACT_FAX	VARCHAR2(20 char)	
CREW_REFERENCE_NUMBER	VARCHAR2(20 char)	
USER_SID	NUMBER(19)	
COUNTRY_OF_BIRTH	VARCHAR2(2)	

WASTE_DISPOSALS

ESTIMATE_GENERATED	NUMBER(19,4)	
MAX_STORAGE	NUMBER(19,4)	
RETAINED_ON_BOARD	NUMBER(19,4)	
TO_BE_DELIVERED	NUMBER(19,4)	
REMAIN_WASTE_DELIVERY_PORT	VARCHAR2(5 char)	
WASTE_TYPE_CODE	VARCHAR2(255 char)	
WASTE_SID	NUMBER(19)	<fk>

SANITARY_MEASURES

HEALTH_SID	NUMBER(19)	<pk,fk>
SANITARY_MEASURE_DT	TIMESTAMP	
SANITARY_MEASURE_PLACE	VARCHAR2(256 char)	
SANITARY_MEASURE_TYPE	VARCHAR2(255 char)	

WASTE_TYPE

CODE	VARCHAR2(255 char)	<pk>
DESCRIPTION	VARCHAR2(255 char)	

CREW_EFFECTS

DESCRIPTION	VARCHAR2(255 char)	
CREW_SID	NUMBER(19)	<fk>
SEQ_NUMBER	VARCHAR2(20 char)	
USER_SID	NUMBER(19)	

CREW_DUTIES

CODE	VARCHAR2(21 char)	<pk>
DESCRIPTION	VARCHAR2(50 char)	

HEALTH_INFECTED_AREAS

HEALTH_SID	NUMBER(19)	<fk1>
DATE_OF_CALL_INFECTED_AREA	TIMESTAMP	
PORT_OF_CALL_INFECTED_AREA	VARCHAR2(5 char)	<fk2>

WASTE_DELIVERY_RECEIPT

SID	NUMBER(19)	<pk,fk>
LOCATION_OR_TERMINAL_NAME	VARCHAR2(255 char)	
RECEPTION_FACILITY_PROVIDER	VARCHAR2(255 char)	
TREATMENT_FACILITY_PROVIDER	VARCHAR2(255 char)	
WASTE_DISCHARGE_FROM	TIMESTAMP(6)	
WASTE_DISCHARGE_TO	TIMESTAMP(6)	

PASSENGERS

SID	NUMBER(19)	<pk>
PASSENGER_NUMBER	VARCHAR2(20 char)	
DATE_OF_BIRTH	TIMESTAMP	
PERSON_FAMILY_NAME	VARCHAR2(256 char)	
PERSON_GIVEN_NAME	VARCHAR2(256 char)	
PLACE_OF_BIRTH	VARCHAR2(256 char)	
TRANSIT	NUMBER(1)	
VISA_NUMBER	VARCHAR2(256 char)	
IDENTITY_DOCUMENT_NATURE	VARCHAR2(17 char)	
IDENTITY_DOCUMENT_NUMBER	VARCHAR2(35 char)	
DISEMBARKATION_PORT	VARCHAR2(5 char)	<fk4>
EMBARKATION_PORT	VARCHAR2(5 char)	<fk3>
NATIONALITY_ID	VARCHAR2(2 char)	<fk2>
SHIP_CALL_SID	NUMBER(19)	<fk1>
BUSINESS_PHONE	VARCHAR2(20 char)	
CONTACT_EMAIL	VARCHAR2(256 char)	
CONTACT_FAX	VARCHAR2(20 char)	
USER_SID	NUMBER(19)	
COUNTRY_OF_BIRTH	VARCHAR2(2 char)	

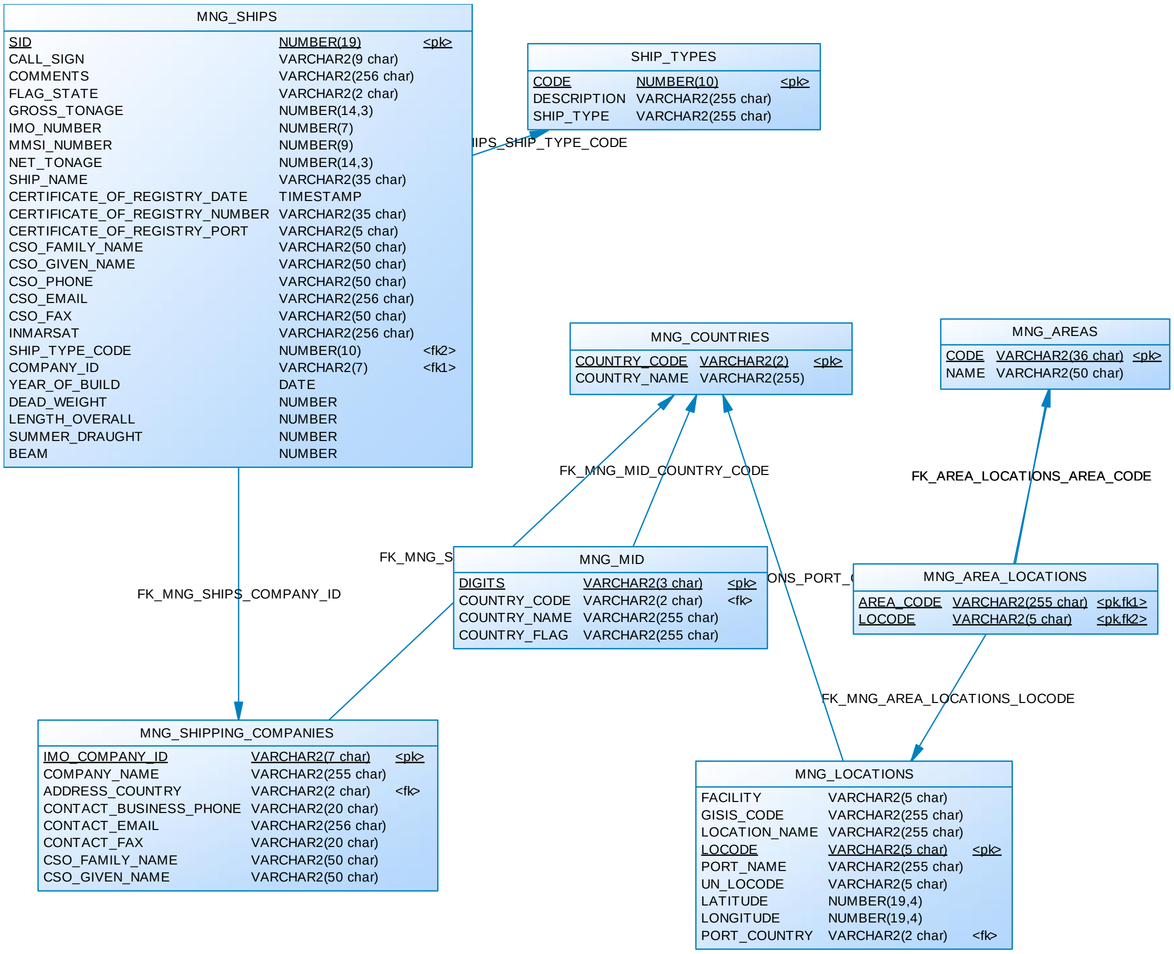
HEALTH_MDH

SID	NUMBER(19)	<pk>
CASE_DISPOSAL	VARCHAR2(255 char)	
COMMENTS	VARCHAR2(255 char)	
EMBARKATION_DT	TIMESTAMP	
GENDER	VARCHAR2(6 char)	
ILLNESS	VARCHAR2(256 char)	
LOCATION_OF_EVACUATION	VARCHAR2(255 char)	
REPORTED_TO_PORT_MEDICAL	NUMBER(1)	
STATE	VARCHAR2(255 char)	
SYMPTOMS_DT	TIMESTAMP	
TREATMENT	VARCHAR2(256 char)	
HEALTH_SID	NUMBER(19)	<fk>
MDH_NUMBER	VARCHAR2(20 char)	
CREW_OR_PASSENGER	NUMBER(1)	
USER_SID	NUMBER(19)	

WASTE_RECEIVED

WASTE_DELIVERY_RECEIPT_SID	NUMBER(19)	<pk,fk>
WASTE_TYPE_CODE	VARCHAR2(256 char)	
WASTE_TYPE_DESCRIPTION	VARCHAR2(256 char)	
QUANTITY_RECEIVED	NUMBER	

Figure 5-4 Ship Calls 4 - Physical Design Diagram



MNG_SHIPS

SID	NUMBER(19)	<pk>
CALL_SIGN	VARCHAR2(9 char)	
COMMENTS	VARCHAR2(256 char)	
FLAG_STATE	VARCHAR2(2 char)	
GROSS_TONAGE	NUMBER(14,3)	
IMO_NUMBER	NUMBER(7)	
MMSI_NUMBER	NUMBER(9)	
NET_TONAGE	NUMBER(14,3)	
SHIP_NAME	VARCHAR2(35 char)	
CERTIFICATE_OF_REGISTRY_DATE	TIMESTAMP	
CERTIFICATE_OF_REGISTRY_NUMBER	VARCHAR2(35 char)	
CERTIFICATE_OF_REGISTRY_PORT	VARCHAR2(5 char)	
CSO_FAMILY_NAME	VARCHAR2(50 char)	
CSO_GIVEN_NAME	VARCHAR2(50 char)	
CSO_PHONE	VARCHAR2(50 char)	
CSO_EMAIL	VARCHAR2(256 char)	
CSO_FAX	VARCHAR2(50 char)	
INMARSAT	VARCHAR2(256 char)	
SHIP_TYPE_CODE	NUMBER(10)	<fk2>
COMPANY_ID	VARCHAR2(7)	<fk1>
YEAR_OF_BUILD	DATE	
DEAD_WEIGHT	NUMBER	
LENGTH_OVERALL	NUMBER	
SUMMER_DRAUGHT	NUMBER	
BEAM	NUMBER	

SHIP_TYPES

CODE	NUMBER(10)	<pk>
DESCRIPTION	VARCHAR2(255 char)	
SHIP_TYPE	VARCHAR2(255 char)	

MNG_COUNTRIES

COUNTRY_CODE	VARCHAR2(2)	<pk>
COUNTRY_NAME	VARCHAR2(255)	

MNG_AREAS

CODE	VARCHAR2(36 char)	<pk>
NAME	VARCHAR2(50 char)	

MNG_MID

DIGITS	VARCHAR2(3 char)	<pk>
COUNTRY_CODE	VARCHAR2(2 char)	<fk>
COUNTRY_NAME	VARCHAR2(255 char)	
COUNTRY_FLAG	VARCHAR2(255 char)	

MNG_AREA_LOCATIONS

AREA_CODE	VARCHAR2(255 char)	<pk,fk1>
LOCODE	VARCHAR2(5 char)	<pk,fk2>

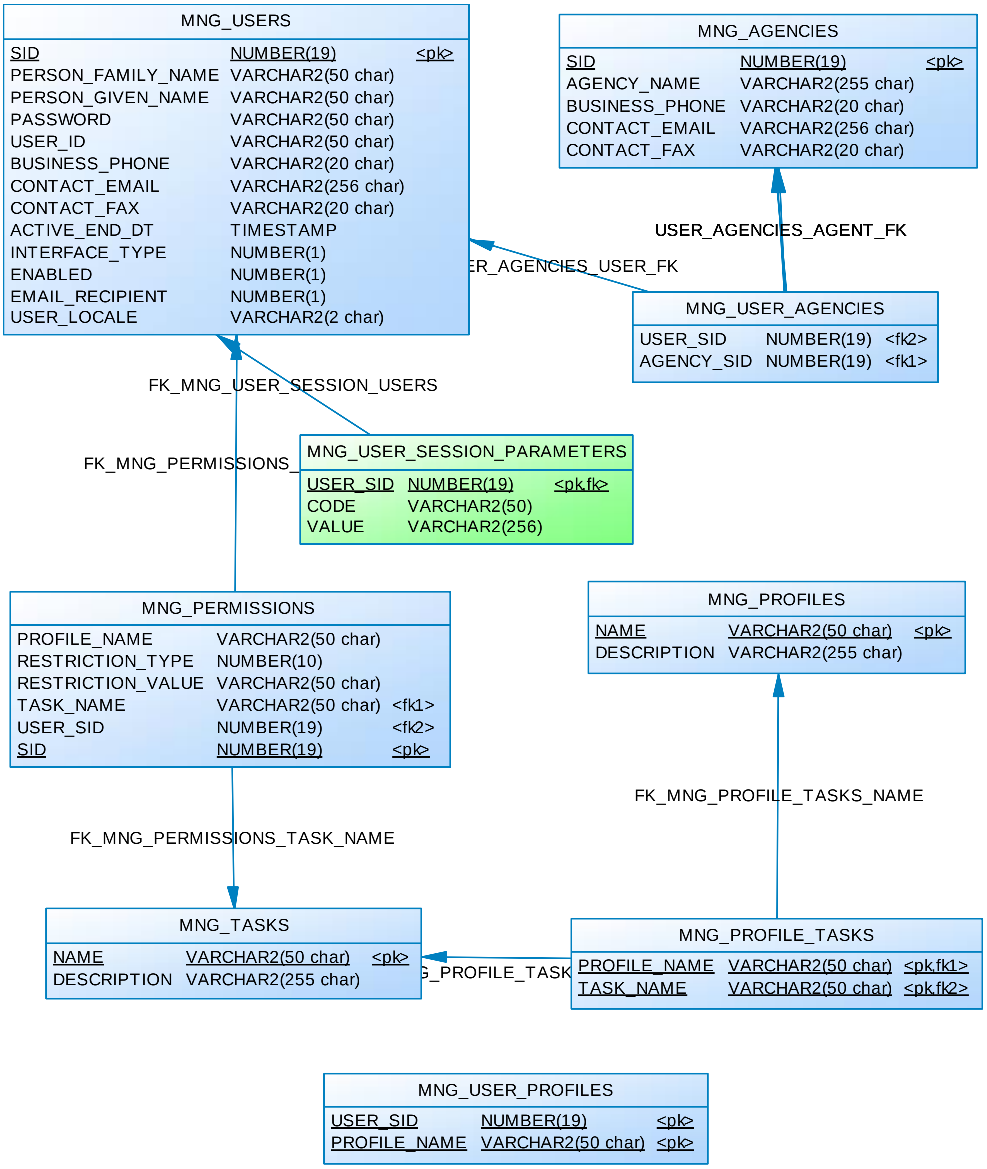
MNG_SHIPPING_COMPANIES

IMO_COMPANY_ID	VARCHAR2(7 char)	<pk>
COMPANY_NAME	VARCHAR2(255 char)	
ADDRESS_COUNTRY	VARCHAR2(2 char)	<fk>
CONTACT_BUSINESS_PHONE	VARCHAR2(20 char)	
CONTACT_EMAIL	VARCHAR2(256 char)	
CONTACT_FAX	VARCHAR2(20 char)	
CSO_FAMILY_NAME	VARCHAR2(50 char)	
CSO_GIVEN_NAME	VARCHAR2(50 char)	

MNG_LOCATIONS

FACILITY	VARCHAR2(5 char)	
GISIS_CODE	VARCHAR2(255 char)	
LOCATION_NAME	VARCHAR2(255 char)	
LOCODE	VARCHAR2(5 char)	<pk>
PORT_NAME	VARCHAR2(255 char)	
UN_LOCODE	VARCHAR2(5 char)	
LATITUDE	NUMBER(19,4)	
LONGITUDE	NUMBER(19,4)	
PORT_COUNTRY	VARCHAR2(2 char)	<fk>

Figure 5-5 Ships and Locations - Physical Design Diagram


USER_AGENCIES_AGENT_FK
ER_AGENCIES_USER_FK
FK_MNG_USER_SESSION_USERS
FK_MNG_PERMISSIONS_
FK_MNG_PERMISSIONS_TASK_NAME
FK_MNG_PROFILE_TASKS_NAME
_PROFILE_TASK

MNG_USERS		
SID	NUMBER(19)	<pk>
PERSON_FAMILY_NAME	VARCHAR2(50 char)	
PERSON_GIVEN_NAME	VARCHAR2(50 char)	
PASSWORD	VARCHAR2(50 char)	
USER_ID	VARCHAR2(50 char)	
BUSINESS_PHONE	VARCHAR2(20 char)	
CONTACT_EMAIL	VARCHAR2(256 char)	
CONTACT_FAX	VARCHAR2(20 char)	
ACTIVE_END_DT	TIMESTAMP	
INTERFACE_TYPE	NUMBER(1)	
ENABLED	NUMBER(1)	
EMAIL_RECIPIENT	NUMBER(1)	
USER_LOCALE	VARCHAR2(2 char)	

MNG_AGENCIES		
SID	NUMBER(19)	<pk>
AGENCY_NAME	VARCHAR2(255 char)	
BUSINESS_PHONE	VARCHAR2(20 char)	
CONTACT_EMAIL	VARCHAR2(256 char)	
CONTACT_FAX	VARCHAR2(20 char)	

MNG_USER_AGENCIES		
USER_SID	NUMBER(19)	<fk2>
AGENCY_SID	NUMBER(19)	<fk1>

MNG_USER_SESSION_PARAMETERS		
USER_SID	NUMBER(19)	<pk,fk>
CODE	VARCHAR2(50)	
VALUE	VARCHAR2(256)	

MNG_PERMISSIONS		
PROFILE_NAME	VARCHAR2(50 char)	
RESTRICTION_TYPE	NUMBER(10)	
RESTRICTION_VALUE	VARCHAR2(50 char)	
TASK_NAME	VARCHAR2(50 char)	<fk1>
USER_SID	NUMBER(19)	<fk2>
SID	NUMBER(19)	<pk>

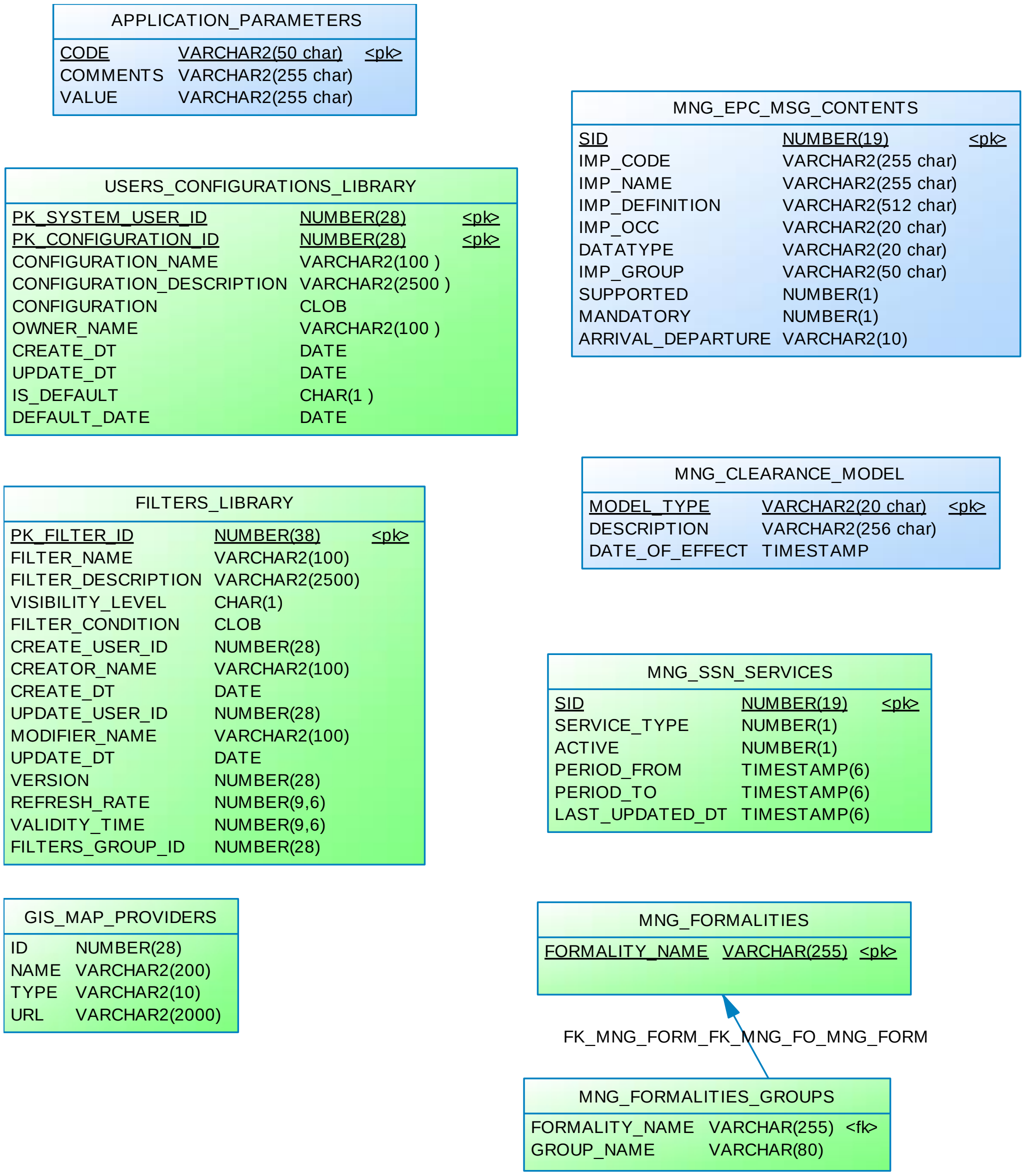
MNG_PROFILES		
NAME	VARCHAR2(50 char)	<pk>
DESCRIPTION	VARCHAR2(255 char)	

MNG_TASKS		
NAME	VARCHAR2(50 char)	<pk>
DESCRIPTION	VARCHAR2(255 char)	

MNG_PROFILE_TASKS		
PROFILE_NAME	VARCHAR2(50 char)	<pk,fk1>
TASK_NAME	VARCHAR2(50 char)	<pk,fk2>

MNG_USER_PROFILES		
USER_SID	NUMBER(19)	<pk>
PROFILE_NAME	VARCHAR2(50 char)	<pk>

Figure 5-6 Users - Physical Design Diagram



APPLICATION_PARAMETERS		
CODE	VARCHAR2(50 char)	<pk>
COMMENTS	VARCHAR2(255 char)	
VALUE	VARCHAR2(255 char)	

MNG_EPC_MSG_CONTENTS		
SID	NUMBER(19)	<pk>
IMP_CODE	VARCHAR2(255 char)	
IMP_NAME	VARCHAR2(255 char)	
IMP_DEFINITION	VARCHAR2(512 char)	
IMP_OCC	VARCHAR2(20 char)	
DATATYPE	VARCHAR2(20 char)	
IMP_GROUP	VARCHAR2(50 char)	
SUPPORTED	NUMBER(1)	
MANDATORY	NUMBER(1)	
ARRIVAL_DEPARTURE	VARCHAR2(10)	

USERS_CONFIGURATIONS_LIBRARY		
PK_SYSTEM_USER_ID	NUMBER(28)	<pk>
PK_CONFIGURATION_ID	NUMBER(28)	<pk>
CONFIGURATION_NAME	VARCHAR2(100)	
CONFIGURATION_DESCRIPTION	VARCHAR2(2500)	
CONFIGURATION	CLOB	
OWNER_NAME	VARCHAR2(100)	
CREATE_DT	DATE	
UPDATE_DT	DATE	
IS_DEFAULT	CHAR(1)	
DEFAULT_DATE	DATE	

MNG_CLEARANCE_MODEL		
MODEL_TYPE	VARCHAR2(20 char)	<pk>
DESCRIPTION	VARCHAR2(256 char)	
DATE_OF_EFFECT	TIMESTAMP	

FILTERS_LIBRARY		
PK_FILTER_ID	NUMBER(38)	<pk>
FILTER_NAME	VARCHAR2(100)	
FILTER_DESCRIPTION	VARCHAR2(2500)	
VISIBILITY_LEVEL	CHAR(1)	
FILTER_CONDITION	CLOB	
CREATE_USER_ID	NUMBER(28)	
CREATOR_NAME	VARCHAR2(100)	
CREATE_DT	DATE	
UPDATE_USER_ID	NUMBER(28)	
MODIFIER_NAME	VARCHAR2(100)	
UPDATE_DT	DATE	
VERSION	NUMBER(28)	
REFRESH_RATE	NUMBER(9,6)	
VALIDITY_TIME	NUMBER(9,6)	
FILTERS_GROUP_ID	NUMBER(28)	

MNG_SSN_SERVICES		
SID	NUMBER(19)	<pk>
SERVICE_TYPE	NUMBER(1)	
ACTIVE	NUMBER(1)	
PERIOD_FROM	TIMESTAMP(6)	
PERIOD_TO	TIMESTAMP(6)	
LAST_UPDATED_DT	TIMESTAMP(6)	

GIS_MAP_PROVIDERS	
ID	NUMBER(28)
NAME	VARCHAR2(200)
TYPE	VARCHAR2(10)
URL	VARCHAR2(2000)

MNG_FORMALITIES		
FORMALITY_NAME	VARCHAR(255)	<pk>

MNG_FORMALITIES_GROUPS		
FORMALITY_NAME	VARCHAR(255)	<fk>
GROUP_NAME	VARCHAR(80)	

Figure 5-7 Configuration and Management entities - Physical Design Diagram

5.2 IMP Tables

This section lists and describes the tables holding the IMP data model definition and are depicted in the diagrams of the previous section.

For the detailed table descriptions please refer to Annex C: Detailed Physical Design Data Model of this document.

Table	Comment
APPLICATION_PARAMETERS	Holds application parameters that define: – The country representing the IMP Demonstrator instance. – The version for the IMP Demonstrator application. – The Authority for the IMP Demonstrator application. – Authority URL for dispatching the original request for clearance message. – The Value for ReplyUri EPC element. – The clearance model.
ATTACHMENTS	It holds file (i.e. binary: picture, PDF, XLS, DOC) of MNG_ATTACHMENT_TYPE. Each attachment is associated with a specific ShipCall and data group.
BUNKERS_REMAINING_ONBOARD	It holds the quantity of bunkers remaining on board the ship reported per ship call.
CALL_PURPOSES	It holds the ship call purpose (EDIFACT codes (8025)) . Part of the Port Call data group.
CARGO_DECLARATIONS	It holds the cargo declaration specific data reported.
CARGO_ITEMS	It holds the list of cargo items per consignment and cargo declaration.
CARGO_ROUTING	It holds the cargo sequence number for a given country.
CIVIL_LIABILITY_CERT_BUNKERS	It holds the certificate of insurance or other financial security in respect of civil liability for bunker oil pollution damage, issued in accordance with the provisions of article 7 of the International Convention on Civil Liability for Bunker Oil Pollution Damage/2001. Reported per ship call.
CIVIL_LIABILITY_CERTS	It holds the certificate of insurance or other financial security in respect of civil liability for oil pollution damage, issued in accordance with the provisions of article VII of the International Convention on Civil Liability for Oil Pollution

Table	Comment
	Damage/1992. Reported per ship call.
CONSIGNMENTS	It holds the consignments reported for a given Cargo Declaration.
CREW	It holds the list of crew members reported per ship call. Amongst data stored are the crew name, duty, nationality visa etc.
CREW_DUTIES	Reference table. It holds the list of possible crew duties defined by a duty code.
CREW_EFFECTS	It holds the crew effects per crew member reported per clearance request notification. Crew effects describe the types of possible dutiable or prohibited items.
CRUISE_SHIP_ITINERARY	It holds the list of ports where the ship is expected to call from the initial departure port to the final arrival port of the cruise, with the corresponding dates and times of expected arrivals per ship voyage.
DPG	It holds the dangerous and polluting goods indication per ship call. Data stored are the INF ship class, confirmation of DPG list on board and cargo manifest contact details.
DPG_ITEMS	It holds the actual list of dangerous and polluting goods reported on board the ship for a given ship call. Amongst data stored are Port of loading, Port of discharge, No. of packages, Package type, DG classification, IMO hazard class etc.
EPC_CLEARANCE_STATUS	It holds per ship call, Authority and data group the clearance status. In case is discarded due to incomplete details, the details are stored in the comments field.
EPC_NOT_MESSAGES	It holds the EPC messages exchanged including: The EPC notification requests. The EPC receipt message. The EPC acknowledgement message send by the Authority information exchange module. Per record the EPC message header data are

Table	Comment
	stored. The XML message contents are stored..
FILTERS_LIBRARY	It contains the GIS Filters defined by every NSW user.
GIS_MAP_PROVIDERS	It contains all GIS layers.
HEALTH	It holds the health information per ship call. Amongst data stored are Exemption or Control Certificate, Visited infected area, Port of call in infected area, Disease on board, Number of ill persons etc
HEALTH_INFECTED_AREAS	It holds the Date of Call and Port of Call in Infected Areas.
HEALTH_MDH	It holds the health information details per crew or passenger on board the ship. Amongst data stored are Embarkation date, Illness Symptoms date, Reported to port medical, State, Case Disposal, Location of evacuation, Treatment etc
INMARSAT_CALL_NUMBERS	It holds the Inmarsat call numbers for the ship reported in a clearance notification.
LAST_TEN_PORT_CALLS	It holds information related to the last 10 calls at port facilities per voyage. Data stored are Port, Port facility Date of arrival, Date of departure, Security level and Special or additional security measures.
MNG_AGENCIES	Resource management table used to hold registry of agencies.
MNG_AREA_LOCATIONS	Resource management table used to hold the actual locations per area defined.
MNG_AREAS	Resource management table used to hold the areas defined as a group of locations within a country.
MNG_ATTACHMENT_TYPES	Resource management table holding the types of attachments.
MGN_CLEARANCE_MODEL	It defines the clearance model supported by the MS (NSW).
MNG_COUNTRIES	Resource management table used to hold the countries registry of the NSW.

Table	Comment
MNG_EPC_MSG_CONTENTS	Resource management table used to hold the set of data elements per group defined in the master file. The National Administrator will select the groups of data elements that will be supported by the NSW The table will be populated during installation. All the elements defined in the master file are stored in this table. For each element the table will store: – Code – Name – Definition – Occasion – Data type and – Group – ARRIVAL_DEPARTURE The column ARRIVAL_DEPARTURE indicates whether the corresponding element must be declared either for ARRIVAL or for DEPARTURE or BOTH. The National Administrator will select/deselect from the list to define those supported by the MS and will be considered when reported in a clearance notification to the MS. These data will be used for the configuration – per MS - of the regulatory information (that is the groups of data elements supported by the MS hence the NSW; SUPPORTED = 1 for true).
MNG_FORMALITIES	Resource management table used to hold the formalities: ENS, FAL2, Summary Declaration for Temporary Storage, eManifest, DPG, FAL7.
MNG_FORMALITIES_GROUPS	Resource management table used to hold the formalities and the associated groups of data elements
MNG_LOCATIONS	Resource management table used to hold the locations registry of the NSW.
MNG_PERMISSIONS	Resource management table used to hold the tasks assigned per user along with the geographical restrictions (where applicable). The permissions define the set of access rights the user has when interfacing with the NSW.
MNG_PROFILE_TASKS	Resource management table used to hold the tasks assigned per profile.
MNG_PROFILES	Resource management table used to hold the

Table	Comment
	definition of profiles (i.e. Ship Data Provider, National Administrator, Authority).
MNG_SHIPPING_COMPANIES	Resource management table used to hold registry of shipping companies.
MNG_SHIPS	Resource management table used to hold the ship registry of the NSW.
MNG_SSN_SERVICES	It holds the SSN CLD and CSD request service parameters.
MNG_TASKS	Resource management reference table storing the tasks defined in the NSW. Tasks are defined as a function (e.g. send) to be performed on a given entity (e.g. clearance notification)
MNG_USER_AGENCIES	Resource management table used to hold the relationship between the users and the agencies. One User may be associated with one or more Agencies.
MNG_USER_PROFILES	Resource management table used to hold the profiles assigned to a user. Even though only one profile is envisaged per user; for future extensions users may be assigned with different roles that require them to use a different profile.
MNG_USER_SESSION_PARAMETERS	It holds the user default search criteria/filters.
MNG_USERS	Resource management table used to hold the user accounts per user/system interfacing the NSW. Every human and system must be identified by a unique user_id.
MOST_RELEVANT_SHIP_CALLS	It holds the most relevant ship calls per ship. To be used by NSW GI. Ship calls with the ETA or ETD closest to current timestamp within the arrival notifications with status = expected and the departure notifications with status = expected. If there is no Ship call with status = expected, the notification with the ATA or ATD closest to current timestamp within the arrival notifications with status = arrived and the departure notifications with status = departed. If there is no ship call with status = expected or arrived or departed, then there is no most relevant ship call.

Table	Comment
PASSENGERS	It holds the list of passengers reported per ship call. Amongst data stored are name, nationality visa etc.
PORT_CALLS	It holds the actual port of stay (in an arrival notification) or the port of departure (in a departure notification. The port call is mandatory information reported for each clearance request and refers to a given ship call defined in the data database. Data stored are Voyage Number (if reported; this is unique per ship, port of call and arrival/departure), ETA to port of call, ETD from port of call, Position in port of call, Name of agent at port of call, Contact details of agent at port of call and Purpose of call.
SANITARY_MEASURES	It holds the valid sanitation control measures related with the health information per ship call.
SECURITY	It holds security related information for the ship reported in the ship call. Amongst data stored are the confirmation of a valid International Ship Security Certificate, if not the reason for no valid ISSC, ISSC, ISSC Type, ISSC issuer, expiration date, Approved security plan on board, Current ship security level etc.
SHIP_CALLS	Per valid clearance request notification received (either via the XML/.SOAP or the Web interface), a ship call record will be created to be stored in this table. The primary identifier is the Journal number that is created for every ship call in the NSW. Every consecutive notification referring to a given ship call will be associated with the ship call identified and stored in this table. This is the master table for the ship call; details reported in the notifications received by the NSW are stored in the dedicated (per group of data elements) table created for that particular purpose in the database (i.e. DPG, PORT_CALL, SECURITY etc). Data stored are: Journal Number, indication of it concerns an arrival or departure, the reported ship identification as well as the registered ship internal identifier, the user id of the 1st notification submitted for the ship call,

Table	Comment
	number of persons on board, the clearance request status, date the record was created and the previous ship call of the ship. Application maps every element defined in the XML message to records saved in MNG_EPC_MSG_CONTENTS.
SHIP_CALLS_HISTORY	It holds the history of ship calls reported. Used to record the history of data group updates per ship call.
SHIP_DEFECTS	It holds information regarding problems that could cause significantly reduced manoeuvrability for a given ship.
SHIP_PARTICULARS	It holds the ship particulars reported in a clearance notification.
SHIP_STORES	It holds the dutiable store items and their quantities that the ship carries per ship call.
SHIP_TO_SHIP_ACTIVITIES	It holds per ship security record the ship-to-ship activities. They are reported in chronological order (most recent first), which were carried out during the last 10 calls at port facilities.
SHIP_TYPES	Reference table storing the ship type codes.
SSN_NOT_MESSAGES	It holds the outgoing PortPlus notification messages send to SSN Central. Per record the message header data are stored. The XML message contents are stored..
SUBSIDIARY_RISKS	It holds the subsidiary risks (packing danger group code as appropriate and as defined in IMDG) per dangerous and polluting goods item reported on board the ship.
USERS_CONFIGURATIONS_LIBRARY	It contains the GIS Configurations defined by every NSW user.
WASTE	It holds data relevant to the ship's waste delivery per ship call. Data stored are: Last port delivered and Date, Waste delivery status, Accurate and correct details and Sufficient onboard capacity.
WASTE_DELIVERY_RECEIPT	It holds the waste delivery receipt per departure ship call.

Table	Comment
WASTE_DISPOSALS	It holds per ship waste delivery the actual waste disposals reported and stored in terms of: Waste type, code and description, Max Storage, Retained on board, Port of delivery of remaining waste and Estimate generated.
WASTE_RECEIVED	It holds the amount of waste received per type of waste related to the waste delivery receipt.
WASTE_TYPE	Reference table storing the definition of the Waste type codes.

Table 5-1 List of IMP Tables

5.3 IMP References

The referential integrity constraints that are based on the relationships among master and detail tables or the relationships between tables and reference data tables please refer to Annex C: Detailed Physical Design Data Model.

6 Deployment view

The NSW deployment view is shown in Figure 6-1.

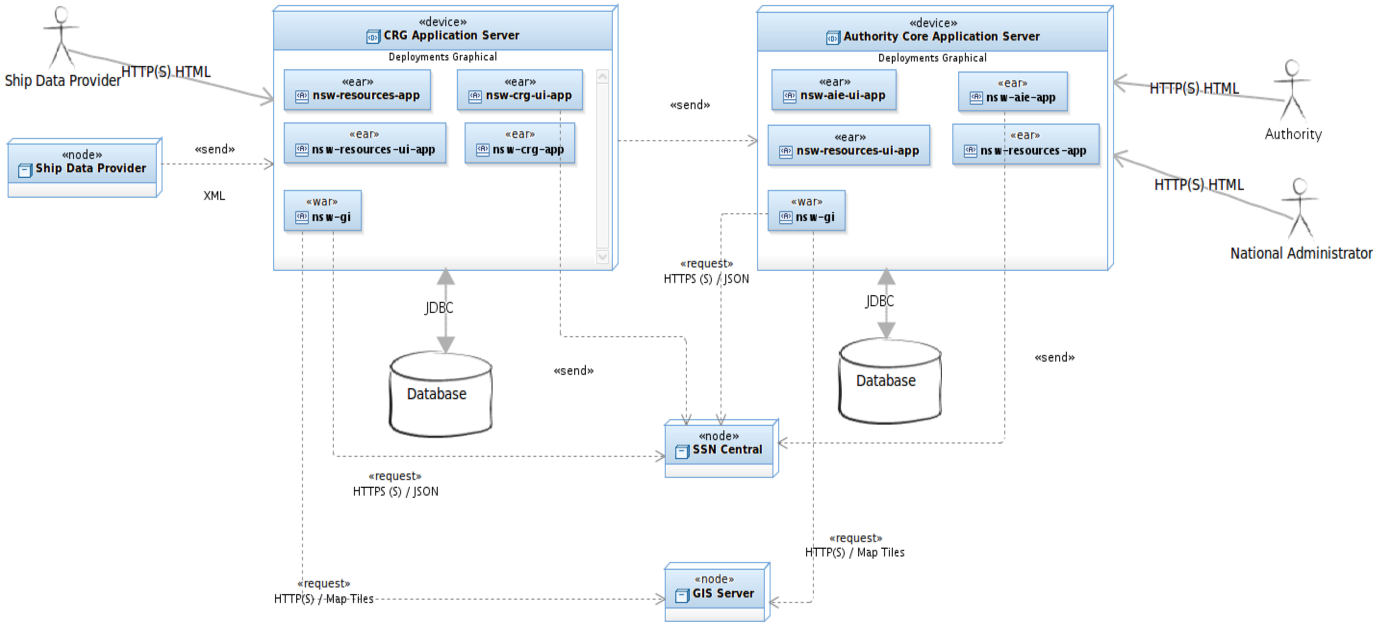


Figure 6-1. NSW Deployment view

6.1 Common Reporting Gateway

The application server hosting CRG artifacts shall be a virtual host running Red Hat Enterprise Linux 5.3 or later.

Technical Platform: CRG artifacts shall be deployed onto a J2EE application server (Oracle WebLogic Server 11g -10.3.6- or alternative Apache Tomcat 7.0.x – 7.0.42). The clustering feature (active/active) may be enabled.

Transaction: The CRG system is transactional, leveraging the technical platform capabilities.

Persistence: Data persistence will be addressed using the Oracle RDBMS (version 11.2.0.3) relational database that stores all data related to CRG.

Deployment artifacts that compose the CRG application at runtime: cgi-core.war and cgi-ui.war.

Java Version: JDK 1.7 (1.7.25) required.

The Deployment artifact cgi-msgapp.war will communicate with

- ➢ Ship Data Providers (system) via HTTP(S) / SOAP or XML messages.
- ➢ Authority system via HTTPS / SOAP or XML messages.
- ➢ Authority system via SMTP messages (via the container mail session).

- SSN system via HTTPS / SOAP or XML messages (ShipCall request/response).
- Local DB via JDBC.

The Deployment artifact cgi-console.war will communicate with

- Ship Data Providers (web user) via HTTP(S) / HTML.

6.2 Authority subsystem

The application server hosting Authority artifacts shall be a virtual host running Red Hat Enterprise Linux 5.3 or later.

Technical Platform: Authority artifacts shall be deployed onto a J2EE application server (Oracle WebLogic Server 11g -10.3.6- or alternative Apache Tomcat 7.0.x – 7.0.42). The clustering feature (active/active) may be enabled.

Transaction: The Authority system is transactional, leveraging the technical platform capabilities.

Persistence: Data persistence will be addressed using the

- Oracle RDBMS (version 11.2.0.3) relational database that stores all data related to CRG.
- Alternatively, PostgreSQL 9.x may be used

Deployment artifacts that compose the Authority application at runtime: authority-information-exchange.war and authority-console.war.

Java Version: JDK 1.7 (1.7.25) required.

The Deployment artifact authority-information-exchange.war will communicate with

- CRG system via HTTPS / SOAP or XML messages.
- SSN system via HTTPS / SOAP or XML messages (PortPlus notification).
- Local DB via JDBC.

The Deployment artifact authority-ui.war will communicate with

- Authority (web user) via HTTP(S) / HTML.
- National Administrator (web user) via HTTP(S) / HTML.

6.3 NSW-GI subsystem

The application server hosting NSW-GI artifacts shall be a virtual host running Red Hat Enterprise Linux 5.3 or later.

Technical Platform: NSW-GI artifacts shall be deployed onto a J2EE application server (Oracle WebLogic Server 11g -10.3.6- or alternative Apache Tomcat 7.0.x – 7.0.42). The clustering feature (active/active) may be enabled.

Transaction: The NSW-GI system is transactional, leveraging the technical platform capabilities.

Persistence: Data persistence will be addressed using the

- Oracle RDBMS (version 11.2.0.3) relational database that stores all data related to NSW-GI.
- Alternatively, PostgreSQL 9.x may be used

Deployment artifacts that compose the NSW-GI application at runtime: nsw-gi.war.

Java Version: JDK 1.7 (1.7.25) required.

The Deployment artifact nsw-gi.war will communicate with

- SSN system via HTTP(S) / JSON.
- GIS server via HTTP(S).
- Local DB via JDBC.

Annex A: Business Rules

Business rules applicable through the processing of clearance request data and the acknowledgements process are listed in the following table. The list will be reviewed during the implementation phase to include any additional business rules applicable.

No	Business Rule	Measures to be taken	Comments
1	A Ship Data Provider can submit a Clearance Notification if he is identified in the NSW and is assigned at least one PROVIDE task.	If the user does not have been assigned the Ship Data Provider profile and the corresponding task for the data groups he/she is reporting then the message is rejected. 1. Receipt message with RequestErrorCode = 5 2. The message will not be forwarded to the authorities and will not cause any further processing (based on ISO 28005 standard).	Error Code 5 -> User does not have to necessary authorisation to provide such request. This may be because the user is unknown, does not have the right to send requests, does not have the right to send request for this port of call, or the request contains data elements that the user does not have the right to include in the request. A description of the BR violation will be included UC-CDP-5
2	The port of call must be within the set of ports the ship data provider covers.	In case of a port of call the ship data provider does not cover: 1. Receipt message with RequestErrorCode = 5 2. The message will not be forwarded to the authorities and will not cause any further processing (based on ISO 28005 standard).	A description of the BR violation will be included The set of geographical permissions (i.e. Country, Area within the country or specific Location) will be defined at the User level via the resource management console and will be applied to all tasks assigned to the user). UC-CDP-5

No	Business Rule	Measures to be taken	Comments
3	The groups of data elements in a Clearance Notification must be within the list of groups the Ship Data Provider is permitted to provide (PROVIDE task).	In case of a group of data elements the ship data provider has no permissions to provide: 1. Receipt message with RequestErrorCode = 5 2. The message will not be forwarded to the authorities and will not cause any further processing (based on ISO 28005 standard).	A description of the BR violation will be included UC-CDP-5
4	A ship data provider can consult, update or re-use a group of data elements of a Ship Call if: - he has been granted the CONSULT task for the group of data elements, and - the Port of Call of the Ship Call is within the geographical restriction applied to the task, and	In different case the application does not display the groups of data elements the user has no read access rights.	UC-RCNWEB-2
5	A ship data provider may be associated with one or more agencies. Information from the following data groups can only be read and/or updated by users associated with the same agency as the ship data provider who submitted the data group. 9. Dangerous and polluting cargo items 10. Security (if the ship security level reported in the notification is 2 or 3) 12. Passengers 13. Crew 14. Crew's Effects 16. Health - MDH Attachment.	In different case the system does not display the data elements of the groups which the user has no read access rights to., and when the notification is received by the system interface, the system rejects the notification	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5, UC-RCNWEB-2
6	If a Clearance Notification reports a Journal Number, it must be a Journal Number that is generated	If not (the JournalNumber is not recorded in the NSW)	Code 4 -> Business rules exceptions. A description of the BR violation will be included.

No	Business Rule	Measures to be taken	Comments
	by the NSW.	the message is rejected. Receipt message with RequestErrorCode = 4	UC-CDP-6
7	A Voyage Number cannot be used for two different ships.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-6
8	Every Clearance Notification shall identify: - the ship (at least one of the ship identification elements "IMO number", "MMSI number", "Call sign", "Ship name" must be defined), - the Port of Call, and - The Ship Call Type (Arrival or Departure).	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5
9	The elements in a clearance notification must be permitted for ARRIVAL or DEPARTURE or both types of a ship call.	Application maps every element defined in the XML message to records saved in MNG_EPC_MSG_CONTENTS. The column ARRIVAL_DEPARTURE indicates whether the corresponding element must be declared either for ARRIVAL or for DEPARTURE or BOTH. In the XML notification message: a) If the mandatory elements for the type of ship call being reported are not provided the message is rejected. b) If Departure elements are reported in an Arrival notification then the Departure elements will be ignored (and vice	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5, UC-RCNWEB-2

No	Business Rule	Measures to be taken	Comments
		versa).	
10	"Port Facility" must be provided if group "Security" is provided.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5
11	"ETA to Port of Call" must be < "ETD from Port of call" if provided.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5
12	Value "ZZOFF" may be used for "Next Port". (This is to be used if the ship is bound to an offshore location)		
13	"ETA to next port" must be > "ATD Port of Call" if provided. "ETA to next port" must be > "ETD from Port of Call" if provided.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5
14	"ATD Port of call" must be > "ATA Port of call" if provided.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5
15	"ATA Port of call" cannot be older than one year	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included UC-CDP-5
16	If the group "Dangerous and polluting cargo items" is provided, then the element "Next Port" and "ETA to Next Port" must be provided. Value "ZZUKN" (Unknown) is accepted as Next Port. In this case, ETA to Next Port is not mandatory.	If not the message is rejected. Receipt message with RequestErrorCode = 3	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-RCNWEB-2, UC-CDP-5
17	If "Visited infected area" = Yes then "Port of call in infected area" and "Date of call in infected area" must be defined.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
18	If "Any person died" = Yes then "Number of deaths" must be defined.	If not the message is rejected. Receipt message with	Code 4 -> Business rules exceptions. A description of the BR violation will be included.

No	Business Rule	Measures to be taken	Comments
		RequestErrorCode = 4	UC-CDP-5
19	If “Sanitary measure” = Yes then “Type of sanitary measure”, “Place of sanitary measure” and “Date of sanitary measure” must be defined.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
20	If “Stowaways” = Yes then “Location stowaways joined ship” must be defined.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
21	If provided, “Number of passengers” must be equal to number of passengers in group “Passengers”.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
22	If provided, “Number of crew” must be equal to number of crew in group “Crew”.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
23	“IMO Hazard Class” must be provided is “DG classification” = “IMDG” or “IGC”.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
24	“UN Number” must be provided is “DG classification” = “IMDG” or “IGC”.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
25	Elements “Max storage”, “Retained on board” and “Estimate generated” must be provided for all waste items if “Waste delivery status” = “Some” or “None”.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
26	“Reason for no valid ISSC” must be provided if “Valid ISSC” = “No”	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
27	In the NSW ship database, a ship is uniquely identified by the IMO Number (not null).	The DB shall not permit duplicate records with the same IMO.	UC-CRM-15
28	In a Clearance Notification, the Port of Call (identified by the Locode of the specific Port location) must belong to the NSW Country.	If not the message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5

No	Business Rule	Measures to be taken	Comments
29	A Clearance Notification cannot be reported with Journal Number that refers to a Ship Call in the NSW DB with Ship Call Status = Closed.	The message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
30	A Clearance Notification cannot be reported without Journal Number and with [Voyage Number, Port of call, Ship Call Type] that refers to a Ship Call in the NSW DB with Ship Call Status = Closed.	The message is rejected. Receipt message with RequestErrorCode = 4	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
31	The NSW must indicate in the receipt message the clearance model adopted by the NSW.	In case of "systematic clearance" or "silent clearance" the receipt message will report where UsesSW = TRUE. In case of "no clearance" the receipt message will report where UsesSW = FALSE.	UC-RCNXML-1
32	Clearance decision can be given only by the relevant authorities of the Ship Call. Relevant Authorities to a Ship Call are the Authorities which are assigned at least one CLEARANCE task which complies to the following: - The task is related to a data group included in the Ship Call, and - The geographical scope of the task includes the Port of Call of the Ship Call.	If not the Web application will not permit the user to select notifications for clearance.	UC-ACK-9, UC-ACK-10
33	A data group of a Ship Call is relevant to an Authority if the Authority is assigned the CLEARANCE task associated to the data group, with a geographical restriction which includes the Port of Call of the Ship Call.	If not the Authority is not permitted to Accept or Not Accept the data group.	UC-ACK-10
34	An Acknowledgment is given the Request Status = "Pending" in all other cases than BR 36 and BR 37.		UC-ACK-10
35	An Acknowledgment is given the		UC-ACK-10

No	Business Rule	Measures to be taken	Comments
	Request Status = "NotAccepted" if it has at least one decision "NotAccepted".		
36	An Acknowledgment is given Request Status = "Accepted" if all data groups relevant for the Authority have a decision "Accepted".		UC-ACK-10

37	The ship IMO Number must be 7 digits and the following formula must return zero (0):
	(IMO Number % 10) - (mainCheckSum % 10) = 0
	Where:
	int mainCheckSum = digits[0] + digits[1] + digits[2] + digits[3] + digits[4] + digits[5].
	digits[0] = substring(0, 1)) * 7;
	digits[1] = substring(1, 2)) * 6;
	digits[2] = substring(2, 3)) * 5;
	digits[3] = substring(3, 4)) * 4;
	digits[4] = substring(4, 5)) * 3;
	digits[5] = substring(5, 6)) * 2;
		If not the notification is rejected.	Code 4 -> Business rules exceptions. A description of the BR violation will be included.
			UC-CDP-5

38	The ship MMSI Number must be 9 digits and the first 3 digits must define a valid maritime identifier digit (MID).	If not the notification is rejected.	Code 4 -> Business rules exceptions. A description of the BR violation will be included. UC-CDP-5
39	A Clearance Notification which updates an existing Clearance Notification can neither change the Ship Call Type, nor the IMO number of the ship.	The notification is rejected.	UC-CDP-6
40	"Voyage Number" cannot be provided through the Web interface	No corresponding field is displayed in the form	UC-RCNWEB-2
41	The Request Status of the notification in the CRG is defined as follows If there is at least one acknowledgment with Request Status "Not accepted", then the Request Status of the notification will be "Not accepted". If there is no acknowledgment		UC-ACK-11

No	Business Rule	Measures to be taken	Comments
	with Request Status "Not accepted", the system will consider the Agencies linked to authority users who are relevant for the notification (as defined in business rule n° 31). If for each agency, there is at least one associated Acknowledgment with Request Status "Accepted", then the Request Status of the notification will be "Accepted". In all other situations, the Request Status of the notification will be "Pending".		
42	The "most relevant notification" (the most relevant notification refers to the most relevant ShipCall) for a ship in relation to a port shall have neither status "closed" nor "cancelled". The "most relevant notification" is established as follows: • The notification with the ETA or ETD closest to now within the arrival notifications with status = "expected" and the departure notifications with status = "expected". • If there is no notification with status = "expected": the notification with the ATA or ATD closest to now within the arrival notifications with status = "arrived" and the departure notifications with status = "departed".	If there is no notification with status = "expected" or "arrived" or "departed", then there is no "most relevant notification".	NSW GI
43	Access rights applied in NSW GI to the ships' position data: • Ship data providers (users with PROVIDE tasks) will have access to ship tracks, if they have contributed to "most relevant notification" for that ship and the status of that notification is not "Closed". • Other users will have access to all ships positions.	If the Ship data providers have not contributed to "most relevant notification" for that ship the ship track will not be displayed.	NSW GI

Annex B: Profiles and Tasks

Profiles define resource limits imposed upon a user account. Access rights to the information and functionalities of the NSW are recorded in the form of user profiles. A single user account can be given one or several user profiles. Three user profiles are defined by default: authority, data provider and national administrator. The following table lists the default profiles by name and description.

Profile Name	Description
NATIONAL_ADMIN	Assigned to the user that will act as the National Administrator. The user(s) assigned the profile NATIONAL_ADMIN can perform the function "MANAGE".
DATA_PROVIDER	Assigned to users that will act as the provider of ship arrival or departure clearance request notifications. The user(s) assigned the profile DATA_PROVIDER can perform the functions "PROVIDE" and "CONSULT".
AUTHORITY	Assigned to users that will act as the clearance provider to a notification submitted by a ship data provider. The user(s) assigned the profile AUTHORITY can perform the functions "CLEARANCE" and "CONSULT".

The following table lists the tasks defined in the IMP demonstrator by name and description.

The task is defined as a function to be performed on a given group of data elements (entity). A user that will be assigned a task will be able to perform the indicated – by the task – action on the group of data elements. Functions are pre-defined based on the action:

- PROVIDE
- CLEARANCE
- CONSULT
- MANAGE

Task Name	Description
USER_MANAGE	Manage user accounts.
PROFILE_MANAGE	Manage profile definition.
REQULATORY_INFO_MANAGE	Manage regulatory information by defining the groups of data elements of interest to the NSW.
SHIP_MANAGE	Manage ship definition.
SHIPPING_COMPANY_MANAGE	Manage shipping companies.
LOCATION_MANAGE	Manage location definition.
AREA_MANAGE	Manage area definition.
AGENCY_MANAGE	Manage Agencies
ATTACHMENT_TYPE_MANAGE	Manage the permitted types for file attachments.
SHIP_IDENTIFICATION_PROVIDE	Permission to provide Ship identification data group elements.
SHIP_PARTICULARS_PROVIDE	Permission to provide Ship particulars data group elements.

Task Name	**Description**
PORT_CALL_PROVIDE	Permission to provide Port call data group elements.
PRE_ARRIVAL_PROVIDE	Permission to provide Pre-arrival 72 hour data group elements.
ARRIVAL_PROVIDE	Permission to provide Arrival data group elements.
DEPARTURE_PROVIDE	Permission to provide Departure data group elements.
VOYAGE_PROVIDE	Permission to provide Voyage data group elements.
DPG_PROVIDE	Permission to provide Dangerous and polluting goods data group elements.
DPG_ITEMS_PROVIDE	Permission to provide Consignment, Cargo item and Cargo item – DPG details data groups elements.
CARGO_PROVIDE	Permission to provide Cargo declaration, Consignment, Consignment – Cargo details, Cargo item and Cargo item – Cargo details data groups elements.
SHIP_STORES_PROVIDE	Permission to provide Ship stores data group elements.
WASTE_PROVIDE	Permission to provide Waste data group elements.
WASTE_DISPOSAL_PROVIDE	Permission to provide Waste disposal information data group elements.
SECURITY_PROVIDE	Permission to provide Security data group elements.
NPOB_PROVIDE	Permission to provide Number of persons on board data group elements.
PASSENGERS_PROVIDE	Permission to provide Passengers data group elements.
CREW_PROVIDE	Permission to provide Crew data group elements.
CREW_EFFECTS_PROVIDE	Permission to provide Crew effects data group elements.
HEALTH_PROVIDE	Permission to provide Health data group elements.
HEALTH_MDH_PROVIDE	Permission to provide Health - MDH Attachment data group elements.
WASTE_RECEIPT_PROVIDE	Permission to provide Waste delivery receipt data group elements.
BUNKERS_PROVIDE	Permission to provide Bunkers remaining on-board data group elements.
LIABILITY_CERTIFICATES_PROVIDE	Permission to provide Civil Liability Certificate for Oil and Bunker Oil Pollution Damage data group elements.
SHIP_DEFECTS_PROVIDE	Permission to provide Ship defects data group elements.
SHIP_IDENTIFICATION_CONSULT	Permission to read Ship identification data group element data.
SHIP_PARTICULARS_CONSULT	Permission to read Ship particulars data group element data.
PORT_CALL_CONSULT	Permission to read Port call data group element data.
PRE_ARRIVAL_CONSULT	Permission to read Pre-arrival 72 hour data group element data.
ARRIVAL_CONSULT	Permission to read Arrival data group element data.
DEPARTURE_CONSULT	Permission to read Departure data group element data.
VOYAGE_CONSULT	Permission to read Voyage data group element data.

Task Name	**Description**
DPG_CONSULT	Permission to read Dangerous and polluting goods data group element data.
DPG_ITEMS_CONSULT	Permission to read Consignment, Cargo item and Cargo item – DPG details data groups element data.
CARGO_CONSULT	Permission to read Cargo declaration, Consignment, Consignment – Cargo details, Cargo item and Cargo item – Cargo details data groups elements.
SHIP_STORES_CONSULT	Permission to read Ship stores data group element data.
WASTE_CONSULT	Permission to read Waste data group element data.
WASTE_DISPOSAL_CONSULT	Permission to read Waste disposal information data group element data.
SECURITY_CONSULT	Permission to read Security data group element data.
NPOB_CONSULT	Permission to read Number of persons on board data group element data.
PASSENGERS_CONSULT	Permission to read Passengers data group element data.
CREW_CONSULT	Permission to read Crew data group element data.
CREW_EFFECTS_CONSULT	Permission to read Crew effects data group element data.
HEALTH_CONSULT	Permission to read Health data group element data.
HEALTH_MDH_CONSULT	Permission to read Health - MDH Attachment data group element data.
WASTE_RECEIPT_CONSULT	Permission to read Waste delivery receipt data group elements.
BUNKERS_CONSULT	Permission to read Bunkers remaining on-board data group elements.
LIABILITY_CERTIFICATES_CONSULT	Permission to read Civil Liability Certificate for Oil and Bunker Oil Pollution Damage data group elements.
SHIP_DEFECTS_CONSULT	Permission to read Ship defects data group elements.
SHIP_IDENTIFICATION_CLEARANCE	Permission to provide approval or denial of clearance for Ship identification data group elements.
PORT_CALL_CLEARANCE	Permission to provide acceptance or not of clearance for Port call data group elements.
DPG_CLEARANCE	Permission to provide acceptance or not of clearance for Dangerous and polluting goods, Consignment, Cargo item and Cargo item – DPG details data groups elements.
CARGO_CLEARANCE	Permission to provide acceptance or not of clearance for Cargo declaration, Consignment, consignment – Cargo details, Cargo item and Cargo item – Cargo details data groups elements.
SHIP_STORES_CLEARANCE	Permission to provide acceptance or not of clearance for Ship stores data group elements.
WASTE_CLEARANCE	Permission to provide acceptance or not of clearance for Waste data group elements.

Task Name	**Description**
SECURITY_CLEARANCE	Permission to provide acceptance or not of clearance for Security data group elements.
NPOB_CLEARANCE	Permission to provide acceptance or not of clearance for Number of persons on board data group elements.
CREW_CLEARANCE	Permission to provide acceptance or not of clearance for Crew data group elements.
HEALTH_CLEARANCE	Permission to provide acceptance or not of clearance for Health data group elements.
WASTE_RECEIPT_CLEARANCE	Permission to provide acceptance or not of clearance for Waste delivery receipt data group elements.
BUNKERS_CLEARANCE	Permission to provide acceptance or not of clearance for Bunkers remaining on-board data group elements.
LIABILITY_CERTIFICATES_CLEARANCE	Permission to provide acceptance or not of clearance for Civil Liability Certificate for Oil and Bunker Oil Pollution Damage data group elements.
SHIP_DEFECTS_CLEARANCE	Permission to provide acceptance or not of clearance for Ship defects data group elements.
MAPVIEW	Permission to access the GIS map graphical interface.

Annex C: Detailed Physical Design Data Model

The detailed definition of table and referential integrity constraints are listed hereunder.

For each table the following items are presented:

- The columns with their data type. There is also an indication if the column is used as part of the Primary Key of the table and/or the Foreign Key or the Unique Key.
- The relationships are described by the Foreign Key constraints.
- A SID specifies an internal system identifier that uniquely identifies a record of a table. SIDs are numeric and generated by an Oracle Sequence.

The detailed definition of table and referential integrity constraints are listed hereunder.

For each table the following items are presented:

- The columns with their data type. There is also an indication if the column is used as part of the Primary Key of the table and/or the Foreign Key or the Unique Key.
- The relationships (references) are described by the Foreign Key constraints.
- A SID specifies an internal system identifier that uniquely identifies a record of a table. SIDs are numeric and generated by a sequence.

IMP Tables

Table APPLICATION_PARAMETERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CODE	X		X	VARCHAR2(50 char)	50
COMMENTS				VARCHAR2(255 char)	255
VALUE				VARCHAR2(255 char)	255

Table ATTACHMENTS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALL_SID		X		NUMBER(19)	19
TYPE_SID		X		NUMBER(19)	19
NAME				VARCHAR2(255 char)	255
DESCRIPTION				BLOB	

Table BUNKERS_REMAINING_ONBOARD

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID		X		NUMBER(19)	19
QUANTITY_OF_HEAVY_FUEL_OIL				NUMBER	
QUANTITY_OF_GAS_OIL				NUMBER	
QUANTITY_OF_MARINE_GAS_OIL				NUMBER	
QUANTITY_OF_MARINE_DIESEL_OIL				NUMBER	
QUANTITY_OF_ANY_OTHER_TYPE_OIL				NUMBER	
BUNKER_DELIVERY_RECEIPT				NUMBER(1)	1

Table CALL_PURPOSES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CODE	X		X	NUMBER(2)	2
DESCRIPTION				VARCHAR2(256)	256
TEXT				VARCHAR2(256)	256

Table CARGO DECLARATIONS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALL_SID		X		NUMBER(19)	19
USER_SID		X		NUMBER(19)	19
LRN				VARCHAR2(25 char)	25
MRN				VARCHAR2(35 char)	35
REPORTING_PARTY_EORI				VARCHAR2(17 char)	17
EU_FIRST_PORT_ARRIVAL				VARCHAR2(5 char)	5
ETA_ENS				TIMESTAMP	

Table CARGO_ITEMS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
CONSIGNMENT_SID		X		NUMBER(19)	19
SEQUENCE_NUMBER			X	NUMBER(5)	5
NUMBER_OF_PACKAGES				NUMBER(8)	8
PACKAGE_TYPE				VARCHAR2(2 char)	2
GROSS_QUANTITY_VALUE				NUMBER(19,4)	19
GROSS_QUANTITY_UNIT				VARCHAR2(255 char)	255
NET_QUANTITY_VALUE				NUMBER(19,4)	19
NET_QUANTITY_UNIT				VARCHAR2(255 char)	255
STOWAGE_POSITION				VARCHAR2(25)	25
TRANSPORT_UNIT_ID				VARCHAR2(17)	17
SHIPPING_MARKS				VARCHAR2(512 char)	512
DESCRIPTION_OF_GOODS				VARCHAR2(256)	256
HS_CODE				VARCHAR2(18 char)	18
MEASURE_CONTENT				VARCHAR2(255 char)	255
MEASURE_UNIT				VARCHAR2(255 char)	255
SEAL_NUMBER				VARCHAR2(35 char)	35
COMMUNITY_STATUS_PROOF				VARCHAR2(255 char)	255
CUSTOM_STATUS				VARCHAR2(3 char)	3
IS_DPG				VARCHAR2(1)	1
TEXTUAL_REFERENCE				VARCHAR2(350 char)	350
DG_CLASSIFICATION				VARCHAR2(255 char)	255
IMO_HAZARD_CLASS				VARCHAR2(7 char)	7
UN_NUMBER				VARCHAR2(4 char)	4
PACKING_GROUP				VARCHAR2(4 char)	4
FLASHPOINT				NUMBER(10,4)	10
MARPOL_POLLUTION_CODE				VARCHAR2(255 char)	255
EMS				VARCHAR2(50 char)	50
ADDITIONAL_INFORMATION				VARCHAR2(256 char)	256

Table CARGO_ROUTING

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CARGO_DECLARATION_SID		X	X	NUMBER(19)	19
COUNTRY		X		VARCHAR2(2 char)	2

Table CIVIL_LIABILITY_CERT_BUNKERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID		X		NUMBER(19)	19
STATUS				VARCHAR2(10)	10
EXPIRY_DATE				TIMESTAMP(6)	6
COMMENTS				VARCHAR2(256)	256

Table CIVIL_LIABILITY_CERTS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID		X		NUMBER(19)	19
STATUS				VARCHAR2(10)	10
EXPIRY_DATE				TIMESTAMP(6)	6
COMMENTS				VARCHAR2(256)	256

Table CONSIGNMENTS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
CARGO_DECLARATION_SID		X		NUMBER(19)	19
PORT_OF_LOADING		X		VARCHAR2(5 char)	5
PORT_OF_DISCHARGE		X		VARCHAR2(5 char)	5
TRANSPORT_DOCUMENT_ID				VARCHAR2(35 char)	35
NUMBER_OF_ITEMS				NUMBER(11)	11
UCR				VARCHAR2(35 char)	35

PLACE_WHERE_CONSIGED				VARCHAR2(255 char)	255
GOODS_RECEIPT_PLACE				VARCHAR2(255 char)	255
CARRIER_COMPANY				VARCHAR2(255 char)	255
CARRIER_ADDRESS				VARCHAR2(255 char)	255
CARRIER_POSTCODE				VARCHAR2(255 char)	255
CARRIER_CITY				VARCHAR2(255 char)	255
CARRIER_COUNTRY				VARCHAR2(2 char)	2
CONSIGNOR_COMPANY				VARCHAR2(255 char)	255
CONSIGNOR_ADDRESS				VARCHAR2(255 char)	255
CONSIGNOR_POSTCODE				VARCHAR2(255 char)	255
CONSIGNOR_CITY				VARCHAR2(255 char)	255
CONSIGNOR_COUNTRY				VARCHAR2(2 char)	2
CONSIGNEE_COMPANY				VARCHAR2(255 char)	255
CONSIGNEE_ADDRESS				VARCHAR2(255 char)	255
CONSIGNEE_POSTCODE				VARCHAR2(255 char)	255
CONSIGNEE_CITY				VARCHAR2(255 char)	255
CONSIGNEE_COUNTRY				VARCHAR2(2 char)	2
NOTIFY_PARTY_COMPANY				VARCHAR2(255 char)	255
NOTIFY_PARTY_ADDRESS				VARCHAR2(255 char)	255
NOTIFY_PARTY_POSTCODE				VARCHAR2(255 char)	255
NOTIFY_PARTY_CITY				VARCHAR2(255 char)	255
NOTIFY_PARTY_COUNTRY				VARCHAR2(2 char)	2
PAYMENT_METHOD				VARCHAR2(3 char)	3
NUMBER_OF_AUTHORISATION				VARCHAR2(255 char)	255
ADDITIONAL_INFORMATION				VARCHAR2(512 char)	512

Table CREW

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
CREW_REFERENCE_NUMB				NUMBER	

ER					
PERSON_FAMILY_NAME				VARCHAR2(256)	256
PERSON_GIVEN_NAME				VARCHAR2(256)	256
BUSINESS_PHONE				VARCHAR2(20)	20
CONTACT_EMAIL				VARCHAR2(256)	256
CONTACT_FAX				VARCHAR2(20)	20
DUTY_CODE		X		VARCHAR2(17)	17
NATIONALITY_ID				VARCHAR2(2)	2
DATE_OF_BIRTH				TIMESTAMP	
PLACE_OF_BIRTH				VARCHAR2(256)	256
IDENTITY_DOCUMENT_NATURE				VARCHAR2(17)	17
IDENTITY_DOCUMENT_NUMBER				VARCHAR2(35)	35
VISA_NUMBER				VARCHAR2(256)	256
USER_SID				NUMBER(19)	19
COUNTRY_OF_BIRTH				VARCHAR2(2)	2

Table CREW_DUTIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CODE	X		X	VARCHAR2(20)	20
DESCRIPTION				VARCHAR2(50)	50

Table CREW_EFFECTS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CREW_SID	X	X	X	NUMBER(19)	19
SEQ_NUMBER	X		X	NUMBER	
DESCRIPTION				VARCHAR2(255)	255
USER_SID				NUMBER(19)	19

Table CRUISE_SHIP_ITINERARY

Code	Primary	Foreign Key	Mandatory	Data Type	Length
PORT_CALLS_SID		X	X	NUMBER(19)	19
PORT_OF_CALL			X	VARCHAR2(5)	5
ETA_TO_PORT_OF_CALL				TIMESTAMP	

Table DPG

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
INF_SHIP_CLASS				VARCHAR2(4 char)	4
CONFIRM_DPG_ON_BOARD				NUMBER(1)	1
CD_FAMILY_NAME				VARCHAR2(50 char)	50
CD_GIVEN_NAME				VARCHAR2(50 char)	50
CD_EMAIL				VARCHAR2(256 char)	256
CD_FAX				VARCHAR2(50 char)	50
CD_PHONE				VARCHAR2(50 char)	50
CD_LOCODE				VARCHAR2(5 char)	5
CD_URI				VARCHAR2(256)	256

Table EPC_CLEARANCE_STATUS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SHIP_CALLS_SID		X		NUMBER(19)	19
AUTHORITY				VARCHAR2(256)	256
DATA_GROUP				VARCHAR2(20)	20
USES_SW				NUMBER(1)	1
REQUEST_STATUS				VARCHAR2(20)	20
COMMENTS				VARCHAR2(256)	256
CREATED_DT				TIMESTAMP	

Table EPC_NOT_MESSAGES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SHIP_MESSAGE_ID				VARCHAR2(256)	256
VERSION				VARCHAR2(10)	10
MESSAGE_TYPE				VARCHAR2(50)	50
REPORTING_SYSTEM				VARCHAR2(50)	50
JOURNAL_NUMBER				VARCHAR2(36)	36
SHIP_CALLS_SID		X		NUMBER(19)	19
USER_SID				NUMBER(19)	19
REPLY_URI				VARCHAR2(256)	256
ARRIVAL_DEPARTURE				NUMBER(1)	1
XML_CONTENT				CLOB	
REQUEST_ERROR_CODE				NUMBER(1)	1
SENT_DT				TIMESTAMP	
SID	X		X	NUMBER(19)	19
REQUEST_PROCESSED				NUMBER(1)	1

Table FILTERS_LIBRARY

Code	Primary	Foreign Key	Mandatory	Data Type	Length
PK_FILTER_ID	X		X	NUMBER(38)	38
FILTER_NAME			X	VARCHAR2(100)	100
FILTER_DESCRIPTION			X	VARCHAR2(2500)	2500
VISIBILITY_LEVEL				CHAR(1)	1
FILTER_CONDITION				CLOB	
CREATE_USER_ID			X	NUMBER(28)	28
CREATOR_NAME			X	VARCHAR2(100)	100
CREATE_DT				DATE	
UPDATE_USER_ID			X	NUMBER(28)	28
MODIFIER_NAME			X	VARCHAR2(100)	100
UPDATE_DT				DATE	
VERSION			X	NUMBER(28)	28

REFRESH_RATE				NUMBER(9,6)	9
VALIDITY_TIME				NUMBER(9,6)	9
FILTERS_GROUP_ID			X	NUMBER(28)	28

Table GIS_MAP_PROVIDERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
ID			X	NUMBER(28)	28
NAME			X	VARCHAR2(200)	200
TYPE			X	VARCHAR2(10)	10
URL			X	VARCHAR2(2000)	2000

Table HEALTH

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
VALID_SCE_CC				NUMBER	
ISSUE_DT				TIMESTAMP	
ISSUE_LOCODE				VARCHAR2(5)	5
VISITED_INFECTED_AREA				NUMBER(1)	1
RE_INSPECTION_REQUIRED				NUMBER(1)	1
ANY_PERSON_DIED				NUMBER(1)	1
NUMBER_OF_DEATHS				NUMBER	
DISEASE_ON_BOARD				NUMBER(1)	1
ILL_PERSONS_GREATER				NUMBER(1)	1
ILL_PERSONS_NUMBER				NUMBER	
ILL_PERSONS_NOW				NUMBER(1)	1
MEDICAL_CONSULTED				NUMBER(1)	1
INFECTION_CONDITION_ON_BOARD				NUMBER(1)	1
LOCATION_STOWAWAYS_JOINED_SHIP				VARCHAR2(255)	255
SICK_ANIMAL				NUMBER(1)	1

Table HEALTH_INFECTED_AREAS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
HEALTH_SID		X		NUMBER(19)	19
PORT_OF_CALL_INFECTED_AREA				VARCHAR2(5)	5
DATE_OF_CALL_INFECTED_AREA				TIMESTAMP	

Table HEALTH_MDH

Code	Primary	Foreign Key	Mandatory	Data Type	Length
HEALTH_SID	X	X	X	NUMBER(19)	19
SEQ_NUMBER	X		X	NUMBER	
GENDER				VARCHAR2(6)	6
EMBARKATION_DT				TIMESTAMP	
ILLNESS				VARCHAR2(256)	256
SYMPTOMS_DT				TIMESTAMP	
REPORTED_TO_PORT_MEDICAL				NUMBER(1)	1
STATE				VARCHAR2(255)	255
CASE_DISPOSAL				VARCHAR2(255)	255
LOCATION_OF_EVACUATION				VARCHAR2(255)	255
TREATMENT				VARCHAR2(255)	255
COMMENTS				VARCHAR2(255)	255
MDH_NUMBER				VARCHAR2(20)	20
CREW_PASSENGER				NUMBER	1
USER_SID				NUMBER(19)	19

Table INMARSAT_CALL_NUMBERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SHIP_PARTICULARS_SID		X		NUMBER(19)	19
INMARSAT_NUMBER				VARCHAR2(50)	50

Table LAST_TEN_PORT_CALLS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
PORT_CALLS_SID		X	X	NUMBER(19)	19
PORT_OF_CALL			X	VARCHAR2(5)	5
PORT_FACILITY				VARCHAR2(4)	4
ATA_TO_PORT_OF_CALL				TIMESTAMP	
ATD_FROM_PORT_OF_CALL				TIMESTAMP	
SECURITY_LEVEL				VARCHAR2(3)	3
ADDITIONAL_SECURITY_MEASURES				VARCHAR2(256)	256

Table MNG_AGENCIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER (19)	19

AGENCY_NAME
BUSINESS_PHONE
			X	VARCHAR2(255)
				VARCHAR2(20)
					255
					20

CONTACT_EMAIL				VARCHAR2(20)	256
CONTACT_FAX				VARCHAR2(50)	20

Table MNG_AREA_LOCATIONS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
AREA_CODE	X	X	X	VARCHAR2(36)	36
LOCODE	X	X	X	VARCHAR2(2)	2

Table MNG_AREAS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CODE	X		X	VARCHAR2(36 char)	36
NAME				VARCHAR2(50 char)	50

Table MNG_ATTACHEMENT_TYPES

Code	Primary	Foreign	Mandatory	Data Type	Length

		Key			
ATTACHEMENT_TYPE	X		X	VARCHAR2(80 char)	80
GROUP_NAME				VARCHAR2(80 char)	80

Table MNG_CLEARANCE_MODEL

Code	Primary	Foreign Key	Mandatory	Data Type	Length
MODEL_TYPE	X		X	VARCHAR2(20 char)	20
DESCRIPTION				VARCHAR2(256 char)	256
DATE_OF_EFFECT				TIMESTAMP	

Table MNG_COUNTRIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
COUNTRY_CODE	X		X	VARCHAR2(255)	255
COUNTRY_NAME				VARCHAR2(255)	255

Table MNG_EPC_MSG_CONTENTS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
IMP_CODE				VARCHAR2(50 char)	50
IMP_NAME				VARCHAR2(50 char)	50
IMP_DEFINITION				VARCHAR2(255 char)	255
IMP_OCC				VARCHAR2(20 char)	20
DATATYPE				VARCHAR2(20 char)	20
IMP_GROUP				VARCHAR2(50 char)	50
SUPPORTED				NUMBER(1)	1
MANDATORY				NUMBER(1)	1
ARRIVAL_DEPARTURE				VARCHAR2(20 char)	20

Table MNG_FORMALITIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length

FORMALITY_NAME	X		X	VARCHAR2(80 char)	80

Table MNG_FORMALITIES_GROUPS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
FORMALITY_NAME	X		X	VARCHAR2(80 char)	80
GROUP_NAME				VARCHAR2(80 char)	80

Table MNG_LOCATIONS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
LOCODE	X		X	VARCHAR2(5)	5
FACILITY				VARCHAR2(255)	255
GISIS_CODE				VARCHAR2(255)	255
LOCATION_NAME				VARCHAR2(255)	255
PORT_NAME				VARCHAR2(255)	255
UN_LOCODE				VARCHAR2(255)	255
LATITUDE				NUMBER	
LONGITUDE				NUMBER	
PORT_COUNTRY		X		VARCHAR2(255)	255

Table MNG_PERMISSIONS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
USER_SID		X	X	NUMBER(19)	19
PROFILE_NAME				VARCHAR2(50)	50
RESTRICTION_TYPE			X	NUMBER(1)	1
RESTRICTION_VALUE				VARCHAR2(50)	50
TASK_NAME		X		VARCHAR2(50)	50

Table MNG_PROFILE_TASKS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
PROFILE_NAME	X	X	X	VARCHAR2(50)	50
TASK_NAME	X	X	X	VARCHAR2(50)	50

Table MNG_PROFILES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
NAME	X		X	VARCHAR2(50)	50
DESCRIPTION				VARCHAR2(255)	255

Table MNG_SHIP_DETAILS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SHIP_ID			X	NUMBER(19)	19

Table MNG_SHIPPING_COMPANIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
IMO_COMPANY_ID	X		X	VARCHAR2(7)	7
COMPANY_NAME				VARCHAR2(255)	255
ADDRESS_COUNTRY				VARCHAR2(2)	2
CONTACT_PHONE				VARCHAR2(20)	20
CONTACT_EMAIL				VARCHAR2(256)	256
CONTACT_FAX				VARCHAR2(20)	20

Table MNG_SHIPS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
IMO_NUMBER				NUMBER(7)	7
MMSI_NUMBER				NUMBER(7)	7
CALL_SIGN				VARCHAR2(9)	9
SHIP_NAME				VARCHAR2(35)	35

FLAG_STATE				VARCHAR2(2)	2
COMPANY_ID		X		VARCHAR2(7)	7
SHIP_TYPE_CODE		X		VARCHAR2(50)	50
GROSS_TONAGE				NUMBER	
NET_TONAGE				NUMBER	
CERTIFICATE_OF_REGISTRY_DATE				TIMESTAMP	
CERTIFICATE_OF_REGISTRY_NUMBER				NUMBER(1)	1
CERTIFICATE_OF_REGISTRY_PORT				VARCHAR2(256)	256
CSO_FIRST_NAME				VARCHAR2(50)	50
CSO_LAST_NAME				VARCHAR2(50)	50
CSO_PHONE				VARCHAR2(20)	20
CSO_EMAIL				VARCHAR2(256)	256
CSO_FAX				VARCHAR2(20)	20
COMMENTS				VARCHAR2(256)	256
YEAR_OF_BUILD				TIMESTAMP	
DEAD_WEIGHT				NUMBER(19)	19
LENGTH_OVERALL				NUMBER(19)	19
BEAM				NUMBER(19)	19

Table MNG_SSN_SERVICES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SERVICE_TYPE			X	NUMBER(1)	1
ACTIVE				NUMBER(1)	1
PERIOD_FROM				TIMESTAMP(6)	
PERIOD_TO				TIMESTAMP(6)	
LAST_UPDATED_DT				TIMESTAMP(6)	

Table MNG_TASKS

Code	Primary	Foreign Key	Mandatory	Data Type	Length

NAME	X		X	VARCHAR2(50)	50
DESCRIPTION				VARCHAR2(255)	255

Table MNG_USER_PROFILES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
USER_SID	X	X	X	NUMBER(19)	19
PROFILE_NAME	X	X	X	VARCHAR2(50)	50

Table MNG_USER_AGENCIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
USER_SID	X	X	X	NUMBER(19)	19
AGENCY_SID	X	X	X	NUMBER(19)	19

Table MNG_USER_SESSION_PARAMETERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
USER_SID	X	X	X	NUMBER(19)	19
CODE			X	VARCHAR2(50)	50
VALUE				VARCHAR2(256)	256

Table MNG_USERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
USER_ID				VARCHAR2(50)	50
LAST_NAME				VARCHAR2(50)	50
FIRST_NAME				VARCHAR2(50)	50
PASSWORD				VARCHAR2(50)	50
BUSINESS_PHONE				VARCHAR2(20)	20
CONTACT_EMAIL				VARCHAR2(256)	256
CONTACT_FAX				VARCHAR2(20)	20

ACTIVE_END_DT				NUMBER(1)	1
INTERFACE_TYPE				NUMBER(1)	1
ENABLED				NUMBER(1)	1
EMAIL_RECIPIENT				NUMBER(1)	1

Table MOST_RELEVANT_SHIP_CALLS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_SID		X	X	NUMBER(19)	19
SHIP_CALL_SID			X	NUMBER(19)	19
ARRIVAL_DEPARTURE				NUMBER(1)	1
SHIPCALL_STATUS				VARCHAR2(255 char)	255
CLEARANCE_STATUS				VARCHAR2(255 char)	255
REPORTED_IMO_NUMBER				VARCHAR2(7 char)	7
REPORTED_MMSI_NUMBER				VARCHAR2(9 char)	9
REPORTED_CALL_SIGN				VARCHAR2(9 char)	9
REPORTED_SHIP_NAME				VARCHAR2(35 char)	35
LAST_PORT				VARCHAR2(5 char)	5
ETD_FROM_LAST_PORT				TIMESTAMP	
PORT_OF_CALL				VARCHAR2(5 char)	5
PORT_FACILITY				VARCHAR2(5 char)	5
ETA_TO_PORT_OF_CALL				TIMESTAMP	
ATA_TO_PORT_OF_CALL				TIMESTAMP	
ETD_FROM_PORT_OF_CALL				TIMESTAMP	
ATD_FROM_PORT_OF_CALL				TIMESTAMP	
NEXT_PORT				VARCHAR2(5 char)	5
ETA_TO_NEXT_PORT				TIMESTAMP	
CREATED_DT				TIMESTAMP	
LAST_NOTIFICATION_DT				TIMESTAMP	

Table PASSENGERS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
PASSENGER_NUMBER				NUMBER	
PERSON_FAMILY_NAME				VARCHAR2(256)	256
PERSON_GIVEN_NAME				VARCHAR2(256)	256
NATIONALITY_ID				VARCHAR2(2)	2
DATE_OF_BIRTH				TIMESTAMP	
PLACE_OF_BIRTH				VARCHAR2(256)	256
IDENTITY_DOCUMENT_NATURE				VARCHAR2(17)	17
IDENTITY_DOCUMENT_NUMBER				VARCHAR2(35)	35
EMBARKATION_PORT				VARCHAR2(5)	5
DISEMBARKATION_PORT				VARCHAR2(5)	5
TRANSIT				NUMBER(1)	1
VISA_RP_NUMBER				VARCHAR2(256)	256
BUSINESS_PHONE				VARCHAR2(20)	20
CONTACT_EMAIL				VARCHAR2(256)	256
CONTACT_FAX				VARCHAR2(20)	20
USER_SID				NUMBER(19)	19
COUNTRY_OF_BIRTH				VARCHAR2(2)	2

Table PORT_CALLS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALL_SID		X		NUMBER(19)	19
VOYAGE_NUMBER				VARCHAR2(5)	5
PORT_OF_CALL				VARCHAR2(5)	5
ETA_TO_PORT_OF_CALL				TIMESTAMP	
ETD_FROM_PORT_OF_CALL				TIMESTAMP	

POSITION_IN_PORT_OF_CALL				VARCHAR2(5)	5
AGENT_AT_PORT_OF_CALL				VARCHAR2(50)	50
AGENT_PHONE				VARCHAR2(20)	20
AGENT_EMAIL				VARCHAR2(256)	256
AGENT_FAX				VARCHAR2(20)	20
PORT_FACILITY				VARCHAR2(5)	5
CARGO_ON_BOARD_DESC				VARCHAR2(256)	256
NEXT_PORT				VARCHAR2(5)	5
ETA_TO_NEXT_PORT				TIMESTAMP	
LAST_PORT				VARCHAR2(5)	5
ETD_FROM_LAST_PORT				TIMESTAMP	
SUBJECT_TO_INSPECTION				NUMBER(1)	1
POSSIBLE_ANCHORAGE				NUMBER(1)	1
PLANED_OPERATIONS				VARCHAR2(256)	256
PLANNED_WORKS				VARCHAR2(256)	256
TANKER_HULL_CONFIG				VARCHAR2(10)	10
CARGO_VOLUME_NATURE				VARCHAR2(256)	256
CARGO_BALLAST_TANK_CONDITION				VARCHAR2(256)	256
ATA_TO_PORT_OF_CALL				TIMESTAMP	
ATD_FROM_PORT_OF_CALL				TIMESTAMP	
AGENT_SID		X		NUMBER(19)	
FORE_DRAUGHT				NUMBER	
MID_SHIP_DRAUGHT				NUMBER	
AFT_DRAUGHT				NUMBER	
AIR_DRAUGHT				NUMBER	

Table PORTCALL_PURPOSES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
PORT_CALLS_SID		X		NUMBER(19)	19
CODE		X		NUMBER(2)	2

Table SANITARY_MEASURES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
HEALTH_SID	X	X	X	NUMBER(19)	19
SANITARY_MEASURE_DT				TIMESTAMP	
SANITARY_MEASURE_PLACE				VARCHAR2(256 char)	256
SANITARY_MEASURE_TYPE				VARCHAR2(255 char)	255

Table SECURITY

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
VALID_ISSC				NUMBER(1)	1
REASON_FOR_NO_VALID				VARCHAR2(256)	256
ISSC_TYPE				VARCHAR2(50)	50
ISSC_ISSUER				VARCHAR2(256)	256
ISSC_ISSUER_TYPE				VARCHAR2(255)	255
ISSC_EXPIRY_DT				TIMESTAMP	
APPROVED_SCC_ON_BOARD				NUMBER(1)	1
CURRENT_SHIP_SECURITY_LEVEL				VARCHAR2(255)	255
SECURITY_RELATED_MATTER				VARCHAR2(256)	256
CSO_FIRST_NAME				VARCHAR2(50)	50
CSO_LAST_NAME				VARCHAR2(50)	50
CSO_PHONE				VARCHAR2(20)	20
CSO_EMAIL				VARCHAR2(256)	256
CSO_FAX				VARCHAR2(20)	20
USER_SID				NUMBER(19)	19

Table SHIP_CALLS

Code	Primary	Foreign Key	Mandatory	Data Type	Length

SID	X		X	NUMBER(19)	19
JOURNAL_NUMBER				VARCHAR2(36 char)	36
ARRIVAL_DEPARTURE				NUMBER(1)	1
SHIP_SID				NUMBER(19)	19
REPORTED_IMO_NUMBER				NUMBER(7)	7
REPORTED_MMSI_NUMBER				NUMBER(9)	9
REPORTED_CALL_SIGN				VARCHAR2(7)	7
REPORTED_SHIP_NAME				VARCHAR2(35)	35
NUMBER_OF_CREW				NUMBER(1)	1
NUMBER_OF_PASSENGERS				NUMBER(1)	1
NUMBER_OF_PERSONS_ON_BOARD				NUMBER(1)	1
STOWAWAYS				NUMBER(1)	1
PREVIOUS_SHIP_CALL_SID				NUMBER(19)	19
SHIPCALL_STATUS			X	VARCHAR2(20)	20
CREATED_DT				TIMESTAMP	

Table SHIP_CALLS_HISTORY

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
USER_ID				VARCHAR2(50 char)	50
DATA_GROUP				VARCHAR2(50 char)	50
ORIGINATOR				NUMBER(1)	1
SHIP_MESSAGE_ID				VARCHAR2(256 char)	256
CREATED_ON			X	TIMESTAMP	

Table SHIP_DEFECTS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SHIP_PARTICULARS_SID		X		NUMBER(19)	19
HULL_INTEGRITY				VARCHAR2(256)	256

MANOEUVRABILITY				VARCHAR2(256)	256
MOORING				VARCHAR2(256)	256
CARGO_HANDLING				VARCHAR2(256)	256
COMMUNICATION				VARCHAR2(256)	256
NAVIGATION				VARCHAR2(256)	256
OTHER				VARCHAR2(256)	256

Table SHIP_PARTICULARS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X	X	NUMBER(19)	19
FLAG_STATE				VARCHAR2(2)	2
MNG_IMO_COMPANY_ID				VARCHAR2(7)	7
COMPANY_NAME				varchar2(70)	70
SHIP_TYPE_CODE				VARCHAR2(50)	50
GROSS_TONAGE				NUMBER	
NET_TONAGE				NUMBER	
CERTIFICATE_OF_REGISTRY_DATE				TIMESTAMP	
CERTIFICATE_OF_REGISTRY_NUMBER				VARCHAR2(35)	35
CERTIFICATE_OF_REGISTRY_PORT				VARCHAR2(5)	5
COMMENTS				VARCHAR2(256)	256
YEAR_OF_BUILD				DATE	
DEAD_WEIGHT				NUMBER	
LENGTH_OVERALL				NUMBER	
SUMMER_DRAUGHT				NUMBER	
BEAM				NUMBER	
COMPANY_PHONE				VARCHAR2(50 char)	50
COMPANY_FAX				VARCHAR2(50 char)	50
COMPANY_EMAIL				VARCHAR2(256 char)	256

Table SHIP_STORES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SHIP_CALLS_SID		X		NUMBER(19)	19
SHIP_STORE_DESCRIPTION				VARCHAR2(35 char)	35
ON_BOARD_LOCATION				VARCHAR2(256 char)	256
MEASURE_CONTENT				NUMBER	
MEASURE_UNIT				VARCHAR2(255 char)	255

Table SHIP_TO_SHIP_ACTIVITIES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SECURITY_SID		X		NUMBER(19)	19
LOCODE		X		VARCHAR2(5)	5
LATITUDE				NUMBER(10)	10
LONGITUDE				NUMBER(10)	10
LOCODE_NAME				VARCHAR2(256)	256
FROM_DT				VARCHAR2(255)	255
TO_DT				VARCHAR2(255)	255
ACTIVITY				VARCHAR2(255)	255
ADDITIONAL_SECURITY_MEASURES				VARCHAR2(255)	255

Table SHIP_TYPES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CODE	X		X	VARCHAR2(50)	50
DESCRIPTION				VARCHAR2(255)	255
SHIP_TYPE				VARCHAR2(255)	255

Table SSN_NOT_MESSAGES

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID		X	X	NUMBER(19)	19
MSGREFID				VARCHAR2(36)	36

VERSION				VARCHAR2(10)	10
SHIPCALL_ID				VARCHAR2(36)	36
USER_SID				NUMBER(19)	19
XML_CONTENT				CLOB	
SENT_DT				TIMESTAMP	
PROCESSED_RESULT				VARCHAR2(20)	20

Table SUBSIDIARY_RISKS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
DPG_ITEMS_SID		X		NUMBER(19)	19
SUBSIDIARYRISKS				VARCHAR2(255)	255

Table WASTE

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X		X	NUMBER(19)	19
SHIP_CALLS_SID		X		NUMBER(19)	19
LAST_PORT_DELIVERED				VARCHAR2(5)	5
LAST_PORT_DELIVERED_DATE				TIMESTAMP	
WASTE_DELIVERY_STATUS				VARCHAR2(255)	255
ACCURATE_AND_CORRECT_DETAILS				NUMBER(1)	1
SUFFICIENT_ON_BOARD_CAPACITY				NUMBER(1)	1

Table USERS_CONFIGURATIONS_LIBRARY

Code	Primary	Foreign Key	Mandatory	Data Type	Length
PK_SYSTEM_USER_ID	X		X	NUMBER(28)	28
PK_CONFIGURATION_ID	X		X	NUMBER(28)	28
CONFIGURATION_NAME			X	VARCHAR2(100)	100
CONFIGURATION_DESCRIPTION				VARCHAR2(2500)	2500
CONFIGURATION				CLOB	

OWNER_NAME			X	VARCHAR2(100)	100
CREATE_DT				DATE	
UPDATE_DT				DATE	
IS_DEFAULT			X	CHAR(1)	1
DEFAULT_DATE				DATE	

Table WASTE_DELIVERY_RECEIPT

Code	Primary	Foreign Key	Mandatory	Data Type	Length
SID	X	X	X	NUMBER(19)	19
LOCATION_OR_TERMINAL_NAME				VARCHAR2(255 char)	255
RECEPTION_FACILITY_PROVIDER				VARCHAR2(255 char)	255
TREATMENT_FACILITY_PROVIDER				VARCHAR2(255 char)	255
WASTE_DISCHARGE_FROM				TIMESTAMP(6)	6
WASTE_DISCHARGE_TO				TIMESTAMP(6)	6

Table WASTE_DISPOSALS

Code	Primary	Foreign Key	Mandatory	Data Type	Length
WASTE_SID	X	X	X	NUMBER(19)	19
WASTE_TYPE_CODE		X		VARCHAR2(50)	50
TO_BE_DELIVERED				NUMBER	
MAX_STORAGE				NUMBER	
RETAINED_ON_BOARD				NUMBER	
REMAIN_WASTE_DELIVERY_PORT				VARCHAR2(2)	2
ESTIMATE_GENERATED				NUMBER	

Table WASTE_RECEIVED

Code	Primary	Foreign Key	Mandatory	Data Type	Length

WASTE_DELIVERY_RECEIPT_SID	X	X	X	NUMBER(19)	19
WASTE_TYPE_CODE				VARCHAR2(256 char)	256
WASTE_TYPE_DESCRIPTION				VARCHAR2(256 char)	256
QUANTITY_RECEIVED				NUMBER	

Table WASTE_TYPE

Code	Primary	Foreign Key	Mandatory	Data Type	Length
CODE	X		X	VARCHAR2(50)	50
DESCRIPTION				VARCHAR2(255)	255

IMP References

Code	Parent Table	Child Table	Cardinality
FK_AREA_LOCATIONS_AREA_CODE	MNG_AREAS	MNG_AREA_LOCATIONS	0..*
ATTACHMENTS_SCID_FK	SHIP_CALLS	ATTACHMENTS	0..*
ATTACHMENTS_ATT_FK	MNG_ATTACHEMENT_TYPES	ATTACHMENTS	0..*
FK_BUNKERS_REMAINING_ONBOARD_SID	SHIP_CALLS	BUNKERS_REMAINING_ONBOARD	0..*
FK_CARGO_DECL_SHIP_CALL_SID	SHIP_CALLS	CARGO_DECLARATIONS	0..*
FK_CARGO_ITEM_CONSGMNT_SID	CONSIGNMENTS	CARGO_ITEMS	0..*
FK_CARGO_ROUTING_COUNTRY	MNG_COUNTRIES	CARGO_ROUTING	0..*
FK_CARGO_ROUTING_DECL_SID	CARGO_DECLARATIONS	CARGO_ROUTING	0..*
FK_CIVIL_LIABILITY_CERT_BUNKERS_SID	SHIP_CALLS	CIVIL_LIABILITY_CERT_BUNKERS	0..*
FK_CIVIL_LIABILITY_CERT_SID	SHIP_CALLS	CIVIL_LIABILITY_CERTS	0..*
FK_CONSGNMNTS_CARGO_DECL_SID	CARGO_DECLARATIONS	CONSIGNMENTS	0..*
FK_CONSGNMNTS_PORT_DISCHARGED	MNG_LOCATIONS	CONSIGNMENTS	0..*
FK_CONSGNMNTS_PORT_LOADING	MNG_LOCATIONS	CONSIGNMENTS	0..*

FK_CREW_CREW_DUTY_ID	CREW_DUTIES	CREW	0..*
FK_CREW_EFFECTS_CREW	CREW	CREW_EFFECTS	0..*
FK_CREW_SHIP_CAL	SHIP_CALLS	CREW	0..*
FK_CRUISE_S_PORT_CAL	PORT_CALLS	CRUISE_SHIP_ITINERARY	0..*
FK_DPG_HIP_CAL	SHIP_CALLS	DPG	0..*
FK_DPG_ITEM_DPG	DPG	DPG_ITEMS	0..*
FK_EPC_CLEA_SHIP_CAL	SHIP_CALLS	EPC_CLEARANCE_STATUS	0..*
FK_EPC_NOT_SHIP_CAL	SHIP_CALLS	EPC_NOT_MESSAGES	0..*
FK_HEALTH_INFECTED_AREA_SID	HEALTH	HEALTH_INFECTED_AREAS	0..*
FK_HEALTH_M_HEALTH	HEALTH	HEALTH_MDH	0..*
FK_HEALTH_SHIP_CAL	SHIP_CALLS	HEALTH	0..*
FK_LAST_TEN_PORT_CAL	PORT_CALLS	LAST_TEN_PORT_CALLS	0..*
FK_LOCATIONS_PORT_COUNTRY	MNG_COUNTRIES	MNG_LOCATIONS	0..*
FK_MNG_FORM_REFERENCE_MNG_FORM	MNG_FORMALITIES	MNG_FORMALITIES_GROUPS	1..*
FK_MNG_USER_SHIP_COMPANIES	MNG_SHIPPING_COMPANIES	MNG_USER_SHIP_COMPANIES	0..*
FK_MNG_USER_USER_ID	MNG_USERS	MNG_USER_SHIP_COMPANIES	0..*
FK_PASSENGE_SHIP_CAL	SHIP_CALLS	PASSENGERS	0..*
FK_PERMISSIONS_TASK_NAME	MNG_TASKS	MNG_PERMISSIONS	0..*
FK_PERMISSIONS_USER_ID	MNG_USERS	MNG_PERMISSIONS	0..*
FK_PORT_CAL_SHIP_CAL	SHIP_CALLS	PORT_CALLS	1..1
FK_PORTCALL_CALL_PURPOSE	CALL_PURPOSES	PORTCALL_PURPOSES	0..*
FK_PROFILE_TASKS_PROFILE_NAME	MNG_PROFILES	MNG_PROFILE_TASKS	0..*
FK_PROFILE_TASKS_TASK_NAME	MNG_TASKS	MNG_PROFILE_TASKS	0..*
FK_PURPOSE_PORT_CALL	PORT_CALLS	PORTCALL_PURPOSES	0..*
FK_SANITARY_MEASURES_HEALTH_SID	HEALTH	SANITARY_MEASURES	0..*
FK_SECURITY_SHIP_CAL	SHIP_CALLS	SECURITY	0..*
FK_SHIP_PAR_INMARSAT	SHIP_PARTICULARS	INMARSAT_CALL_NUMBERS	0..*
FK_SHIP_PAR_SHIP_CALL	SHIP_CALLS	SHIP_PARTICULARS	0..*
FK_SHIP_STO_SHIP_CAL	SHIP_CALLS	SHIP_STORES	0..*

FK_SHIP_TO_SECURITY	SECURITY	SHIP_TO_SHIP_ACTIVITIES	0..*
FK_SSN_NOT_EPC_NOT	EPC_NOT_MESSAGES	SSN_NOT_MESSAGES	1..1
FK_SUBSIDIA_DPG_ITEM	DPG_ITEMS	SUBSIDIARY_RISKS	0..*
FK_USER_PROFILES_PROFILE_NAME	MNG_PROFILES	MNG_USER_PROFILES	0..*
FK_USER_PROFILES_USER_ID	MNG_USERS	MNG_USER_PROFILES	0..*
FK_VESSELS_COMPANY_ID	MNG_SHIPPING_COMPANIES	MNG_SHIPS	0..*
FK_VESSELS_SHIP_TYPE_CODE	SHIP_TYPES	MNG_SHIPS	0..*
FK_WASTE_DINF_WASTE_ID	WASTE	WASTE_DISPOSALS	0..*
FK_WASTE_DEL_REC_RECEIVED_SID	WASTE_DELIVERY_RECEIPT	WASTE_RECEIVED	0..*
FK_WASTE_DEL_RECEIPT_SHIPCALL_SID	SHIP_CALLS	WASTE_DELIVERY_RECEIPT	0..*
FK_WASTE_SHIP_CAL	SHIP_CALLS	WASTE	0..*
FK_WASTE_DISPOSALS_WASTE_SID	WASTE_TYPE	WASTE_DISPOSALS	0..*