Appendix B
to Tender Specifications

Technical Specifications of CARD

1 Introduction

The Central Access Rights Database (CARD) is the repository of the policies that govern the access to the SafeSeaNet (SSN) Ecosystem services.

The typical user of the SSN Ecosystem has limited access to the information and services which are provided by the Ecosystem, for example viewing the position of a ship at a given moment in time or the possibility to report information regarding dangerous goods on board a ship. The amount and type of information made available by the user's access rights can be restricted by a data access policy. Restrictions on the access to data are implemented by means of data filtering ("limitation") and limitations vary according to the sensitivity of the information or service to be protected.

Some examples of access rights and limitations on the data are:

- Users of EU Coastal Stations can only see T-AIS ship positions provided by the Member States of the European Union and EFTA.
- A Port authority can only see and provide voyage information for ships bound and calling locations covered by its port.
- A user with profile "Pollution Control" operator may report Incident Reports of type "POLREP" only.

Access rights and limitations are configured and stored in the CARD which makes them available to the SSN Ecosystem's Maritime Applications for enforcement. Limitations are based on the user's Profile and may be dependent on the attributes of the user account, like its Country and its Organization.

The Bidder of this Tender is requested to propose a solution to configure, store, enforce and make available the Access Rights policies to the Maritime Applications that are part of the SSN Ecosystem at EMSA. The solution shall meet the technical specifications set in this document.

The solution should preferably:

- be based on an existing Commercial Off The Shelf product (COTS) which is already available and well established on the market of digital information access protection;
- require a relatively small effort in terms of customization and bespoke software development;
- be based on public industrial standards in the market of digital information access protection;
- be based on IT technology that is easy to deploy and maintain in the existing EMSA IT environment;
- be easily accessible by client systems with a limited integration effort;
- be easy to configure by the EMSA staff without specific IT or software development skills.

The choice of an existing product shall be justified with evidence of the operational use of such a product (case studies) in order to guarantee its reliability and robustness as well as to reduce the CARD testing and acceptance effort.

The Bidder should be aware that the terminology used in this document is based on internal EMSA documents and may differ from the applicable industrial standards.[1]

[1] As an example in other contexts the terms "Profile" and "Role" may have different meanings and refer to "set of permissions", "access to a function" or "access to a resource".

2 TABLE OF CONTENTS

3 Background

This section describes the business environment and underlying systems that will connect to and make use of the CARD.

3.1 The SSN ecosystem

The Maritime Applications of the SSN Ecosystem (e.g. SafeSeaNet, CleanSeaNet, Thetis and EU LRIT Data Center) have been developed to address specific needs defined by distinct legal texts. As a result each Maritime Application handles its specific set of data, user community and access rights mechanisms.

Experience has been gained and technical advancements have been made, in particular in developing an interoperable data exchange system which can combine information from SafeSeaNet with information from the other Union monitoring and tracking systems: CleanSeaNet, the European Union Long-Range Identification and Tracking of Ships European Data Centre (EU LRIT Data Centre) and Thetis. External systems (e.g. Satellite AIS) also provide additional source of information and further enable integrated maritime services. Several satellite AIS initiatives have been launched, including by Member States, confirming the operational benefits from having access to SAT-AIS data.

The EMSA hosted systems and applications are able to provide Member States' authorities and Union bodies, comprehensive information on, for example, ship positions, dangerous cargoes, pollution, etc., as well as provide support services in areas such as anti-piracy and statistics, in accordance with the access rights attributed.

Annex III to Directive 2002/59/EC has been adapted with the Directive 2014/100/EU, to reflect these technical advancements made in light of experience gained with SafeSeaNet. Annex III which covers the Union Maritime Information and Exchange system herein referred as SSN Ecosystem refers to other relevant Union legislation, specifying those Union acts in regard to which SafeSeaNet is currently used, such as Directive 2000/59/EC, Directive 2005/35/EC, Directive 2009/16/EC and Directive 2010/65/EU including space-based technologies.

With such integrated approach it has become necessary to develop a flexible user rights management that allows Member States and/or the EMSA Administrator to specify granular access to the different types of users of the SSN Ecosystem according to the users' profiles and the corresponding access rights. The objective is to set up a Common Management Console (CMC) which will offer an integrated access right and centralized user account configuration and therefore avoid duplication of access right mechanisms. The purpose is to facilitate the development of integrated services, as well as offer a better control of access to the resources of the SSN Ecosystem.

CARD is the module of the CMC system that stores and makes available the user's access rights policies used within the SSN Ecosystem.

3.2 Common Management Console

The Common Management Console (CMC) provides a tool to manage the users, the access rights and the reference information of the SSN Ecosystem.

The high-level architecture diagram of the CMC is shown in Figure 1.

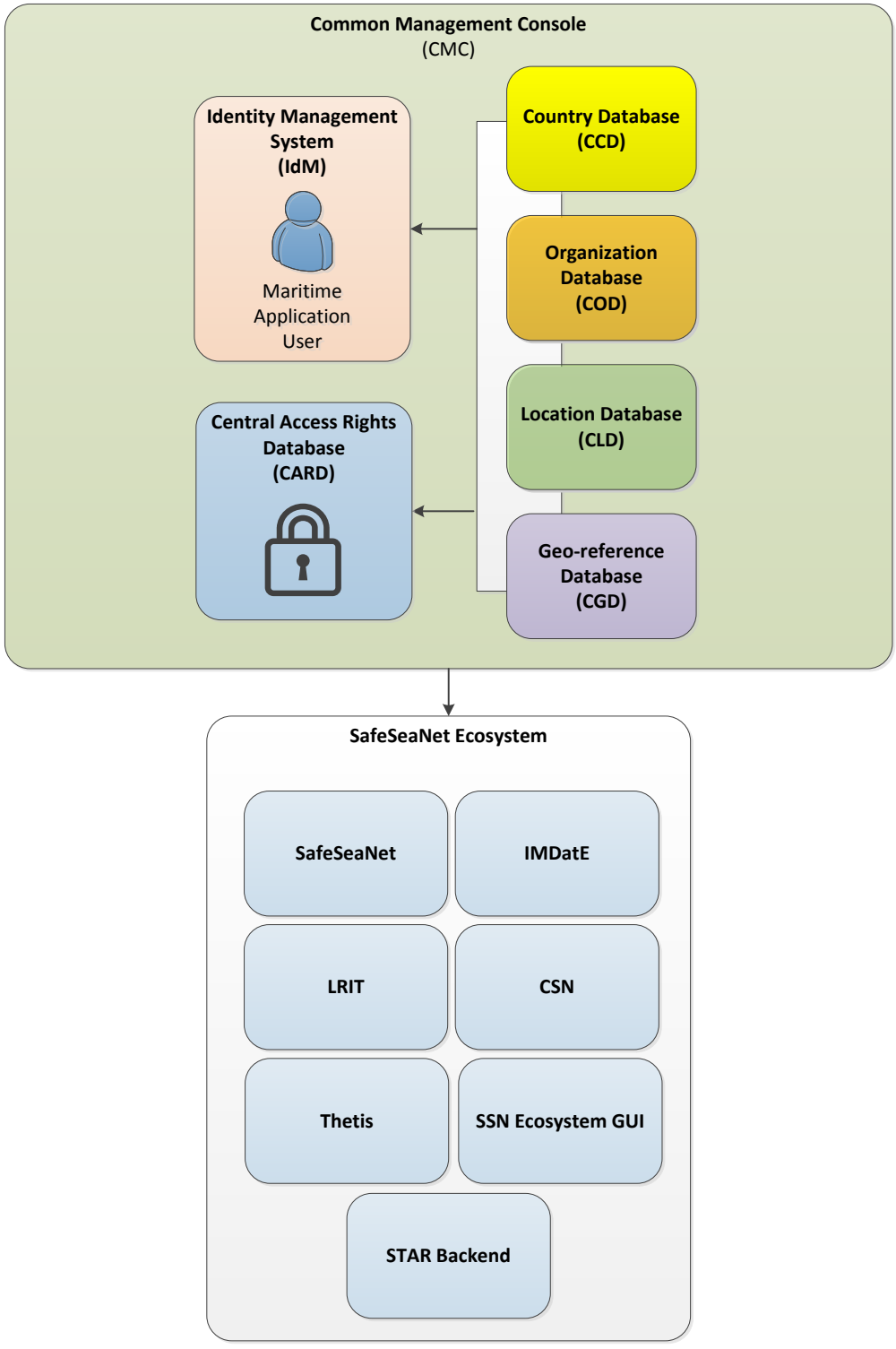


Figure 1 - CMC Architecture

The relevant CMC modules for the CARD project are:

- Identity Management (IdM),
- Central Databases:
    - Central Country Database (CCD),
    - Central Organization Database (COD),

- Central Location Database (CLD),
- Central Geo-reference Database (CGD).

3.2.1 Identity Management (IdM)

An EMSA Administrator creates user accounts of SSN Ecosystem's Maritime Applications with the Identity Management (IdM) module which, similarly to CARD, is also part of the CMC. IdM is the tool to create and manage user accounts at EMSA and it provides the following functions:

- Create and update a user account,
- Provide the user account details to external applications.

CARD is connected to the IdM and evaluates an access right policy based on the user account attributes: Profile(s), Country, Organization and Operations (see section 5 and section 11.1).

Important Note: The development and configuration tasks of the IdM are part of a separate contract and are out of the scope of this Tender.

3.2.2 Central Databases

The Central Databases are repositories of reference information which is used within the SSN Ecosystem. The Central Databases provide unique reference codes to identify commonly used entities such as countries, geographical locations, geographical areas, organisations, etc.

The Central Databases that are relevant for the CARD are:

- Central Country Database (CCD), for Countries and International Institutions;
- Central Organization Database (COD), for administrative entities, authorities, private organisations, etc.,
- Central Location Database (CLD), for geographical locations;
- Central Geo-reference Database (CGD), for geographical areas.

The CARD is connected to the Central Databases above in order to retrieve and identify in a unique way the information items used to configure the access rights policies (see section 11.2).

Important Note: The development and configuration tasks of the Central Databases are part of separate contracts and are out of the scope of this Tender.

4 High-level User Requirements

The CARD is a system that meets several high-level requirements, as defined by the EMSA business units. This section describes the overall aim of the CARD project while the detailed specifications of CARD are provided in the following chapters.

4.1 Protection of Maritime Information

CARD responds to the main business needs of protecting the Maritime Information and making it available to all the authorized users.

The SSN Ecosystem applications store and provide maritime information for safety, security, and anti-pollution purposes. The information (resource) is stored in digital format and can be accessed by external users through a web interface (web based application) or via a system to system interface.

For the sake of clarity, the term *resource* is used in this document to describe an information item of the SSN Ecosystem's Maritime Application that needs to be protected.

Some examples of Maritime Information are:

- Ship Position: latitude, longitude, timestamp, ship identification, and other attributes,
- Voyage information: information related to the voyage of a ship to a port of call and its stay in the port (identification of the port of call, estimated and actual date and time of arrival, estimated and actual date and time of departure, position in the port of call, dangerous and polluting goods on board, etc.),
- Satellite Image: geo-located digital image of the sea surface and/or shoreline, times of acquisition, detected vessels, and other attributes.

Most of the Maritime Information in the SSN Ecosystem is sensitive and access has to be limited according to EU regulations, international or bi-lateral agreements, as well as contracts between EMSA and its data providers.

4.2 The function of CARD

CARD is a software application that provides the following main tools and functions:

- a tool to maintain the list of Services provided by the SSN Ecosystem applications;
- a tool to maintain the list of user Profiles;
- a tool to maintain the list of Roles that give access to resources to be protected;
- a tool to define the access rights policies based on:
    - a user Profile or a combination of user Profiles,
    - the user details (e.g. Country, Organization, Operations);
- a centralized storage of the access right policies;
- a distribution service of the access right policies to other systems;
- an authorization service.

4.3 High Availability

CARD is a critical system for the SSN Ecosystem. If the data access policies are not available, users cannot be authorized to access the Maritime Information and cannot perform their tasks anymore.

See section 12 for the detailed high-availability specifications.

5 Data Access Policy

A Data Access Policy is a set of rules that define the level of protection of a resource. A policy grants to a user access to a specific resource. If the access is granted, the policy also determines the possible limitations based on the user's Country, Organization and Operations. The limitations are built on one or more attributes of the resource to be protected:

- its source,
- its geographical position,
- its associated *location*[2],
- its type, or
- its associated operation.

Note that not all the attributes are relevant to all resources (for example, the position of the ship has no Location or Operation attribute).

Examples of data access policies are provided below:

Sample Policy #1	**EU coastal stations can see T-AIS data from EU and EFTA Member States**
Profile	"Costal Station" operator
Access to Resource	View Ship T-AIS Position
Source limitation	EU, EFTA countries

Sample Policy #2	**A local port authority can only see the exemptions regarding calls in the locations covered by its jurisdiction.**
Profile	"Port" operator
Access to Resource	View Exemptions
Location limitation	Exemptions regarding ships calling a port under the jurisdiction of the User's Organization

The definition of the data access policy can be represented by means of a matrix in which the columns are the user Profiles and the rows are the functions used to access specific resources ("Roles"). Each cell of the matrix contains the information if the Profile (column) includes a particular Role (row). If the Role is not included in the Profile, the cell is empty. If the Role is included, the cell shows the Limitations that will be applied. The preliminary configuration of user Profiles, Roles and Limitations is available in Appendix E to the Tender Specifications.

Figure 2 shows an excerpt of the data access policy matrix where the Profile "Pollution Control" operator (1st column) includes the Role "View METOCEAN Data" without any Limitation (sign "X") and it does not include "View pleasure boat data". In the 2nd column instead the Profile "Coastal Station" operator is associated to both Roles but

[2] The term "location" in the SSN Ecosystem refers to a port or a port facility.

in the case of “View pleasure boat data” there is a Limitation: the user can only view pleasure boat data from his/her country (the letter “S” stands for data “source”).

Role / Profile	Pollution control	Coastal Station
View METOCEAN Data	X	X
View pleasure boat data		S: country

Figure 2 - Example of a Profile-Role-Limitations matrix

The following sections describe the concepts and reference information used within CARD to configure, store and evaluate the data access policies. The list of attributes and values are indicative and are meant to be used by the Bidder to understand and assess the data policy definition and configuration requirements. The complete and detailed list of attributes, values, format and filtering tools will be defined during the Design Phase of the CARD project.

The reference information stored in CARD is also used by the IdM and other modules of the SSN Ecosystem and it should be easily accessible via a system-to-system interface (see section 9.3).

Some mock-ups are also included in order to represent in a more understandable way the type of information and the corresponding management tools and workflows.

Important Note: The aim of the mock-ups is to provide a visual representation of the relevant information fields and tools; the Bidder may propose a different design and implementation given that the functional, performance and usability requirements are met. The final design of the CARD forms and tools will be agreed with EMSA during the Design phase of the CARD project.

5.1 Service

Service is the term used to identify one or more applications that provide access to the SSN Ecosystem’s resources. Examples of Services that are currently part of the SSN Ecosystem are: SSN, LRIT, THETIS, IMS, EOS, etc.

The CARD stores the list of Services provided by the SSN Ecosystem. Each service has a unique alphanumeric identifier (“Service Code”) and a name.

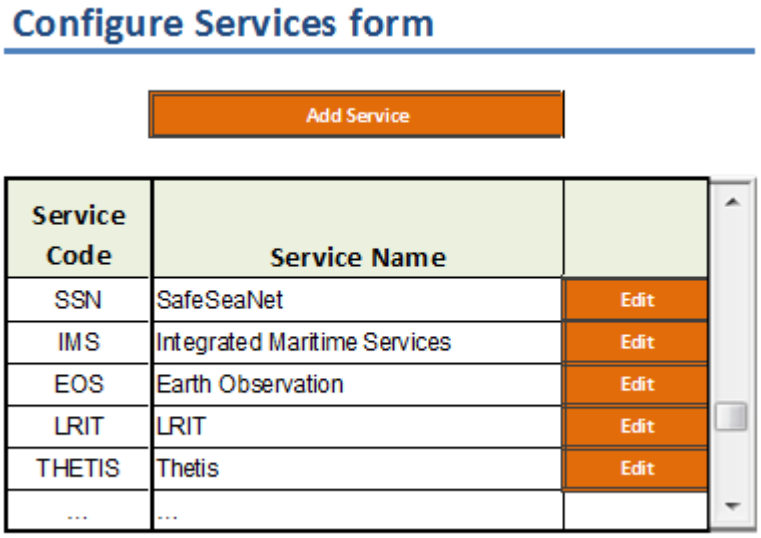
5.1.1 Service attributes

Maximum number of Services: 500.

Attribute	Type	Description	Example
Service Code	String `"^[A-Z0-9_]+$"`	Unique Identifier of the Service, used as reference in the SSN Ecosystem (primary key)	“SSN” “IMS_MS”

Service Name	String	Unique and human-readable name of the Service	“SafeSeaNet” “Integrated Maritime Services to Member States”

5.1.2 Service Configuration form (mock-up)



Req. 1. CARD provides a function to configure and store the list of Services.

5.2 Profile

A Profile describes the high level function of a user of the SSN Ecosystem. Typical examples are “Coastal Station” operator or “Search And Rescue” operator. A Profile provides access to one or more resources, subject in some cases to limitations.

When creating or editing a user account in the IdM module, the Administrator associates it to one or more Profiles according to the user’s functions and tasks within his/her organization.

5.2.1 Profile attributes

Maximum number of Profiles: 1000.

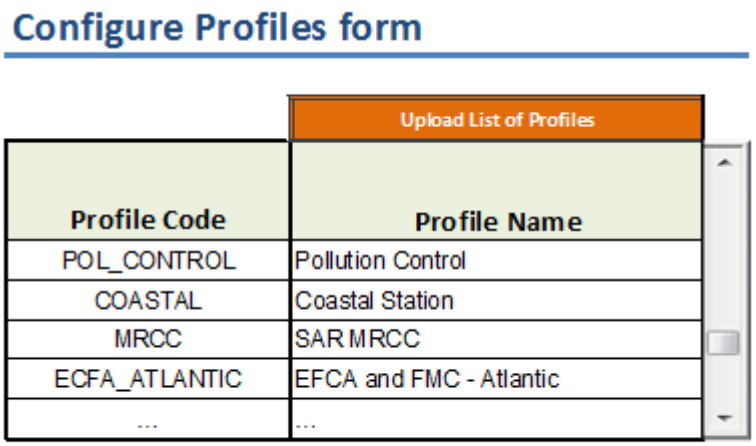
Attribute	Type	Description	Example
Profile Code	String `"^[A-Z0-9_]+$"`	Unique Identifier of the Profile, used as reference in the SSN Ecosystem (primary key)	“SAR” “CST”

Profile Name	String	Unique and human-readable name of the Profile	“Search And Rescue” “Coastal Station”
Profile Group **(optional)**	String	The group to which this Profile belongs to.	“Administration”

CARD stores the list of Profiles and each Profile is identified by a unique code.

The Bidder should also consider the need of grouping Profiles to help the CARD Administrator during the policy configuration.

5.2.2 Profile Configuration form (mock-up)



5.2.3 Profile Filter

CARD provides a “Profile selection tool” that can be used by the CARD Administrator during the Policy configuration.

The Profile selection tool filters the list of Profiles according to the following criteria:

- by Profile Name

- by Profile Code

- by Profile Group

Req. 2.	CARD provides a function to configure, store and filter the list of Profiles.

5.3 Operation

An Operation is a label that is applied to information items of the SSN Ecosystem. The Operation groups the information in categories for access control purposes.

For example, an Earth Observation image may be tagged with the Operation “SAFEMED”. A user can view this image only if he/she is associated with the Operation “SAFEMED”.

When creating or editing a user account in the IdM module, the Administrator associates it to one or more Operations according to the user’s functions and tasks within his/her organization.

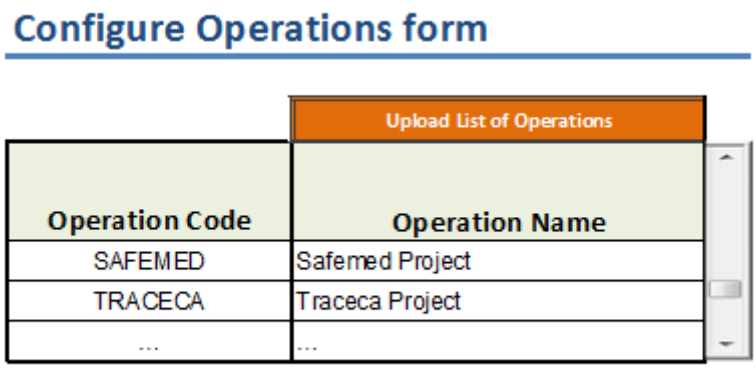
5.3.1 Operation attributes

Maximum number of Operations: 1000.

Attribute	Type	Description	Example
Operation Code	String `"^[A-Z0-9_]+$"`	Unique Identifier of the Operation, used as reference in the SSN Ecosystem (primary key)	“SAFEMED”
Operation Name	String	Unique and human-readable name of the Operation	“SafeMed Project”

CARD stores the list of Operations and each Operation is identified by a unique code.

5.3.2 Operation Configuration form (mock-up)



Req. 3. CARD provides a function to configure and store the list of Operations.

5.4 Roles

A role describes the access to a resource that is available in the SSN Ecosystem. Examples of roles are “View Ship T-AIS Position” or “Provide SSN Port Call”.

5.4.1 Role attributes

Maximum number of Roles: 10.000.

The special attributes “resourceHas…” indicate if a Role refers to a resource that has specific attributes that are relevant for the implementation of the data access policy.

If all “resourceHas…” are set to FALSE, the Role refers to a “simple resource”. If at least one of the “resourceHas…” attributes is set to TRUE, the Role refers to a “complex resource” that has its own attributes: source, location (LOCODE), geographical coordinates, operation, data type (see section 5.4.2).

Attribute	Type	Description	Example
Role Code	String `"^[A-Z0-9_]+$"`	Unique Identifier of the Role, used as reference in the SSN Ecosystem (primary key)	PROVIDE_INCIDENT
Role Name	String	Unique and human-readable name of the Role	“Provide SSN Incident Report”
Service Code	<Service_Code>	Reference to the Service which this role belongs to (see section 5.1)	“SSN”
resourceHasSource	TRUE/FALSE	Indicates if the Role refers to a resource that is made available by a specific identified source	TRUE
resourceHasLocation	TRUE/FALSE	Indicates if the Role refers to a resource that is associated to one or more locations	TRUE
resourceHasCoordinates	TRUE/FALSE	Indicates if the Role refers to a resource that is geolocated, i.e. is associated to a point with coordinates latitude / longitude	TRUE

resourceHasOperations	TRUE/FALSE	Indicates if the Role refers to a resource that is part of an Operation	TRUE
resourceHasDataTypes	TRUE/FALSE	Indicates if the Role refers to a resource which is of different types	TRUE
Description **(optional)**	Text	A description of the data or functions that a user can perform. Optional attribute.	“Send reports on accidents and incidents which have occurred at sea (as per Directive 2002/59/EC) and on ships which have not delivered their ship-generated waste and cargo residues (as per Directive 2000/59/EC)”
Data Types **(optional)**	List of <Data_Type_Code>	The list of Data Types that characterize this Role. Optional attribute.	“PROVIDE_INCIDENT.WASTE”, “PROVIDE_INCIDENT.SITREP”
Operations **(optional)**	List of <Operation_Code>	The list of Operations that the resource referred by this Role is part of. Optional attribute.	SAFEMED, CLEANSEANET
Security Model Level **(optional)**	<Security_Model_Level_Code>	The Security Model level associated to this Role (used by IdM). Optional attribute.	“EMSA_SERVICE_ADMIN”

The configuration of a role may include the setting of Data Types (see section 5.7). Data Types can only be set for Roles that have the attribute resourceHasDataTypes = TRUE.

The configuration of a role may include the setting of Operations (see section 5.3). Operations can only be set for Roles that have the attribute resourceHasOperations = TRUE.

The “Security Model Level” is used by the IdM to set the visibility of the Profiles associated to this Role and it is configured and stored in CARD.

5.4.2 Resource Attributes

As shown in the Role Attribute table, a Role may refer to one of the following two categories of resources.

- **Simple Resource**: a basic type of information or function that the user can fully access or not at all; a Simple Resource does not have any specific attribute: the Role is sufficient to identify all the *simple resources* that it refers to.

For example, the Role "View METOCEAN data" refers to all available meteorological resources (information layers). The "METOCEAN data" is a Simple Resource and the user can either view all the METOCEAN information layers or none at all.

- **Complex Resource**: a complex type of information or function that the user can access with different levels of limitations; a Complex Resource has one or more attributes that are checked by CARD in order to define the level of access limitation for a given user.

For example, the Role "View VMS data" refers to the positions of fishing vessels; this resource has "source" and "coordinates" attributes that are checked by CARD. It is a complex resource and a user may access it only for some source countries or in some specific geographical areas.

A Complex Resource has one or more of the following attributes.

Attribute	**Type**	**Description**	**Example**
Source **(optional)**	<Country_Code>	Country Code that identifies the source of the resource (from CCD)	IT
Location **(optional)**	<Location_Code>	Code of the location associated to the resource (from CLD), generally defined with a UN/LOCODE.	FRLEH
Coordinates.Lat **(optional)**	String "^[+-][0-9]{2}(\.[0-9]{1,6})?$"	The Latitude of the coordinates of the resource.	-12.123456
Coordinates.Lon **(optional)**	String "^[+-][0-9]{3}(\.[0-9]{1,6})?$"	The Longitude of the coordinates of the resource.	+123.123456
Operation **(optional)**	<Operation_Code>	The code of the Operation to which the resource is associated to (from CARD).	"Safemed"
Data Type **(optional)**	<Data_Type_Code>	The code of the Data Type of this resource (from CARD).	PROVIDE_INCIDENT.WASTE

CARD does not store the list of resources and their attributes. The Authorization Service of CARD however responds to requests from a Maritime Application and evaluates the resource attributes provided as request parameters (see section 9.4). CARD therefore needs to compare the values of the relevant attributes with the Data

Access Policies applicable to the user account before granting or denying access to a resource as explained in section 9.

5.4.3 Role Configuration form (mock-up)

Configure Roles form

Add Role

Role Code	Role Name	Service	Description
VIEW_SAT_AIS	IMS View SAT-AIS	IMS	View Sat-AIS position reports
PROVIDE_INCIDENT	SSN Provide Incident Report	SSN	…
VIEW_LRIT_FLAG	LRIT Flag View	LRIT	…
VIEW_EOS_ACTIVITY	EOS View Activity Detection	EOS	…
…	…	…	…

Figure 3 - Role Configuration (part 1)

Configure Roles form

Role Code	Complex Resource	Data Type	Operation	Security Model Level	Action
VIEW_SAT_AIS	hasAttributes				Edit
PROVIDE_INCIDENT		Types			Edit
VIEW_LRIT_FLAG				EMSA_SERVICE_ADMIN	Edit
VIEW_EOS_ACTIVITY			Operations		Edit
…					Edit

Figure 4 - Role Configuration (part 2)

5.4.4 Role Filter

CARD provides a “Role selection tool” that can be used by the CARD Administrator during the Data Access Policy configuration.

The Role selection tool filters the list of Roles according to the following criteria:

1. by Role Name
2. by Role Code
3. by Service
4. by Operation (associated to the resource referred by the Role)
5. if the Role refers to a resource with Data Types or not
6. by Security Model Level

Req. 4.	CARD provides a function to configure, store, and filter the list of Roles.

5.5 Country

The term Country in the SSN Ecosystem refers to the following entities:

- A geopolitical **region or territory**, as defined in ISO 3166, e.g. Portugal;
- An international **institution**, e.g. EMSA;
- A **virtual country**, e,g, “International Waters”
- The category **Company**, which indicates a private enterprise (country code: “XI”).

A user of the SSN Ecosystem is associated to one, and only one, Country.

The list of Countries is stored in the CCD and each Country is identified by a unique 2-char code, e.g. “PT”.

5.5.1 Country attributes

Maximum number of Countries: 1000

Attribute	Type	Description	Example
Country Code	String "^[A-Z0-9]{2}$"	The 2-char code of the Country	“PT”
Country Category	<Country_Category_Code>	The category of Country as defined in the CCD. One of the following values: Company, Country, Institution, Regional Agreement, Virtual Country	“Institution”
Country Type **(optional)**	<Country_Type_Code>	The type of Country as defined in the CCD. Currentlly it may be one of the following values: EEA EFTA EU Acceding Country EU Candidate Country EU Member State European Union Flag State Overseas Territory	“EFTA”

Regional Agreement **(optional)**	List of <Regional_Agreement_Code>	A Country may have signed one or more Regional Agreements among the following that are currently available: Barcelona Black Sea Commission Bonn Agreement HELCOM Paris MoU Wetrep	"HELCOM"
Country Name	String	The name of the Country or Institution	"Portugal"

The CCD provides the following information by means of an export function:

- the list of Countries and their attributes,
- the list of Country Categories,
- the list of Country Types,
- the list of Regional Agreements.

CARD imports the information provided by the CCD into a local read-only copy and uses it to filter a list of Countries and evaluate the data access policies, whenever there is a reference to a Country or a group of Countries. During the import CARD shall check if there are inconsistencies with the existing policies. In case of problems, the CARD Admin has to be warned about the type of inconsistency and the update procedure can be stopped.

5.5.2 Country Filter

CARD provides a "Country selection tool" that can be used by the CARD Administrator during the Policy configuration.

The Country selection tool filters the list of Countries according to the following criteria:

- by Country Name
- by Country Code
- by Country Category
- by Country Types
- by Regional Agreements

Req. 5. CARD uses the list of Countries, Country Types, and Regional Agreements provided by CCD for data access policy configuration and evaluation (see section 6.2)

Req. 6. CARD provides a function to import and update the list of Countries, Country Types, and Regional Agreements used by CARD.

5.6 Organization

The term Organization in the SSN Ecosystem refers to the following entities:

- An office of a public organization within a country, e.g. the “Italian Coast Guard” headquarter in Rome,
- A representation office of an international institution, e.g. the IMO Headquarter,
- The headquarter of a private organization or company.

A user of the SSN Ecosystem is associated to one, and only one, Organization.

The list of Organizations is stored and maintained in the COD and each Organization is identified by a unique code.

5.6.1 Organization attributes

Maximum number of Organizations: 100.000

Attribute	Type	Description	Example
Country Code	<Country_Code>	The Country or Institution which the Organization is associated to.	“PT”
Organization Code	String "^ORG_[A-Z0-9]{2}[0-9]{5}$"	The unique code that identifies the Organization.	”ORG_PT12345”
Parent Organization Code **(optional)**	<Organization_Code>	The code of the parent Organization in the COD hierarchy.	”ORG_PT12344”
Organization Name	String	The name of the Organization	“Lisbon Port Administration”
Organization Type	String	The type of Organization. • Public • Private	Public

Locations **(optional)**	List of <Location_Code>	The list of Locations associated with this Organization	PTLIS, PTALM
Geographical Areas **(optional)**	List of <Area_Code>	The list of Geographical Areas associated with this Organization (area polygons are stored in the CGD)	GEO_123456
Profiles **(optional)**	List of <Profile_Code>	The list of Profiles that the User Administrators of this Organization may assign (from CARD).	“POL_CONTROL”, “MRCC”

The COD provides, by means of a specific service, the details of a particular Organization, the list of Organizations and other relevant information in a pre-defined format.

CARD imports and uses the information provided by the COD for data access policy configuration and evaluation, whenever there is a reference to an Organization in the policy, e.g. a limitation based on a group of Organizations or the user’s organization.

The Bidder should propose a synchronization strategy on how the CARD retrieves and uses the COD information taking into consideration the size and structure of the COD database as well as the CARD availability and performance requirements. During the sync CARD checks if there are inconsistencies with the existing policies. In case of problems, the CARD Administrator is warned about the type of inconsistency and the sync procedure can be stopped.

5.6.2 Organization Filter

CARD provides an “Organization selection tool” that can be used by the CARD Administrator during the Policy configuration.

The Organization selection tool filters the list of Organizations according to the following criteria:

- by Country
- by Organization Name
- by Organization Code
- by Organization Type
- by Parent Organization

Req. 7. CARD uses the Organization information provided by COD for data access policy configuration and evaluation (see section 6.2).

Req. 8. CARD provides a function to keep in sync the Organization information used by the CARD.

5.6.3 Organization – Profile relationship

User Administrators belonging to an Organization may have limited visibility of Profiles. The CARD Administrator configures the list of the Profiles that can be assigned by the User Administrators of an Organization. The Organization-Profile relationship is used by the IdM to limit the access of User Administrators.

5.6.3.1 Organization - Profile Configuration form (mock-up)

Configure Organization - Profile

Filter Organization

Organization Code	Organization Name	Organization Type	Country Code	Profiles	Action
ORG_IT12345	Italian Coast Guard	National Authority	IT		Add Profiles
ORG_FR23416	Port of Le Havre	Local Authority	FR	Profiles	Edit Profiles
ORG_BE34231	MIK	Local Authority	BE		Add Profiles
ORG_XI23464	ExactEarth	Contractor	XI		Add Profiles
	...	...			Add Profiles

Edit Organization-Profiles form

Organization: ORG_PT12345

Profiles

Add Profile

Profile Code	Profile Name	Action
POL_CONTROL	Pollution Control	Remove
MRCC	SAR MRCC	Remove
...	...	

Req. 9. CARD provides a function to configure and store the relationship between Organization and Profiles.

5.7 Data Types

The resources available in the SSN Ecosystem can be characterized using different types.

As an example, an Incident Report has one of the following data types: Waste, SITREP, POLREP, Lost and found containers, Failed to notify, VTS rules infringement, Banned ship, Insurance failure, Pilot or port report, Other.

CARD uses Data Types to define fine-grained limitations on the access to data. Countries and Organizations may have access to limited types of data.

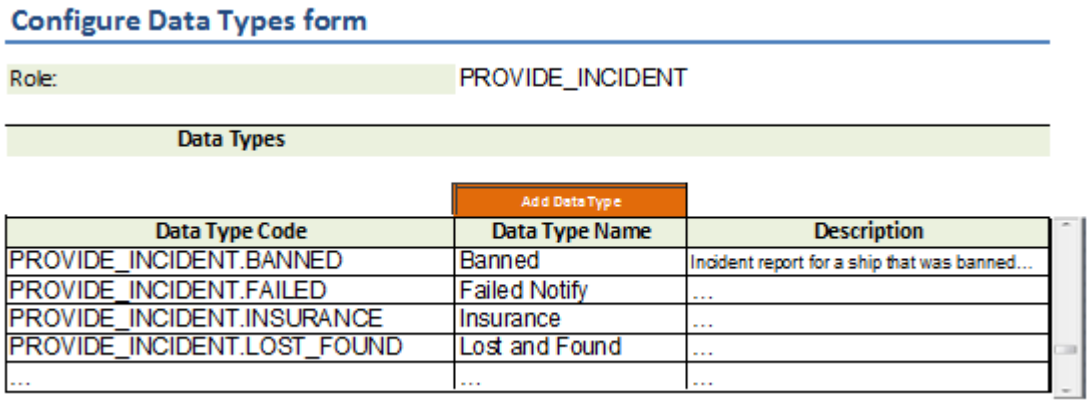
Data Types are associated to a specific Role and the code of the corresponding Role is the prefix of the Data Type code.

5.7.1 Data Type attributes

Maximum number of Data Types per Role: 100

Attribute	Type	Description	Example
Role Code	<Role_Code>	A reference to the Role to which this Data Type is associated (see section 5.4)	“PROVIDE_INCIDENT”
Data Type Code	String "^[A-Z0-9_.]+$" (Note the dot character)	Unique Identifier of the Data Type, used as reference in the SSN Ecosystem (primary key). It is built using the relevant Role as a prefix.	“PROVIDE_INCIDENT.BANNEDSHIP”
Data Type Name	String	Human-readable name of the Data Type. Unique for the relevant Role.	“Banned Ship”
Description **(optional)**	Text	A description of the type of data or functions that a user can access with this role.	“Report regarding a ship which has been refused access to ports of the Member States according to article 16 of Directive 2002/59/EC”

5.7.2 Data Types Configuration form (mock-up)



5.7.3 Data Type Selection tool

CARD provides a “Data Type selection tool” that can be used by the CARD Administrator during the Data Access Policy configuration.

The Data Type selection tool filters the list of Data Types according to the following criteria:

- by Data Type Name

- by Data Type Code
- by Role

Req. 10.	CARD provides a function to configure and store the list of Data Types associated to a Role.

5.7.4 Country – Data Type relationship

Users belonging to a Country may have limited access to some Data Types. The CARD Administrator configures the list of the Data Types that can be accessed by the users of a Country.

5.7.4.1 Country - Data Types Configuration form (mock-up)

Configure Country - Data Type

Filter Country

Country Code	Country Name	Country Category	Country Type	Regional Agreements	Data Type	Action
AL	Albania	Country				Add Data Types
IE	Ireland	Country	EU Member State, EEA, European Union		Types	Edit Data Types
US	USA	Country				Add Data Types
XR	Frontex	Institution				Add Data Types
...	...	...	...	...	...	Add Data Types

Edit Country-Data Types form

Country: IE

Data Types

Add Data Type

Data Type Code	Data Type Name	Action
PROVIDE_INCIDENT.BANNED	Banned	Remove
EOS_IMAGE.HI_RES	High Resolution	Remove
...	...	

Req. 11.	CARD provides a function to configure and store the relationship between Country and Data Types.

5.7.5 Organization – Data Type relationship

Users belonging to an Organization may have limited access to some Data Types. The CARD Administrator configures the list of the Data Types that can be accessed by the users of an Organization.

5.7.5.1 Organization - Data Types Configuration form (mock-up)

Configure Organization - Data Type

Filter Organization

Organization Code	Organization Name	Organization Type	Country Code	Data Type	Action
ORG_IT12345	Italian Coast Guard	National Authority	IT		Add Data Types
ORG_FR23416	Port of Le Havre	Local Authority	FR	Types	Edit Data Types
ORG_BE34231	MIK	Local Authority	BE		Add Data Types
ORG_XI23464	ExactEarth	Contractor	XI		Add Data Types
	...	...			Add Data Types

Edit Organization-Data Types form

Organization: ORG 123

Data Types

Add Data Type

Data Type Code	Data Type Name	Action
PROVIDE_INCIDENT.BANNED	Banned	Remove
EOS_IMAGE.LOW_RES	High Resolution	Remove
...	...	

Req. 12. CARD provides a function to configure and store the relationship between Organization and Data Types.

5.8 Geographical Area

The set of Geographical Areas (“Areas”) used within the SSN Ecosystem are stored in the CGD. Each Area is identified by a unique code.

Areas are divided in several categories based on their geometrical shape: Bounding Box, Polygon, Polygon Set, Circle, etc.

5.8.1 Area attributes

Maximum number of Areas: 100.000

Attribute	Type	Description	Example
Area Code	String `"^[A-Z0-9_]{4,20}$"`	The alphanumeric code of the Area	“GEO_123456”
Area Type	String	The type of the Area	“TSS”,

	"^[A-Z0-9_]{3,20}$"		“COASTAL_1000_NM”
Area Category	String	The category of the Area: BBOX, Polygon, …	“BBOX”
Area Name	String	The name of the Area	“Baltic Sea”
Country **(optional)**	<Country_Code>	The Country which the Area is associated to	“PT”
Organization **(optional)**	<Organization_Code>	The Organization which the Area is associated to	“ORG_PT12345”

The CGD provides the following information by means of an export function:

- the list of Areas (set of bounding boxes and polygons) and their attributes,
- the list of Area Types,
- the list of Area Categories.

CARD uses the information provided by the CGD to filter a list of Areas, configure and evaluate the data access policies, whenever there is a reference to an Area.

The Bidder should propose a synchronization strategy on how the CARD retrieves and uses the CGD information taking into consideration the size and structure of the CGD database as well as the CARD availability and performance requirements. During the sync CARD checks if there are inconsistencies with the existing policies. In case of problems, the CARD Administrator is warned about the type of inconsistency and the sync procedure can be stopped.

5.8.2 Area Filter

CARD provides an “Area selection tool” that can be used by the CARD Administrator during the Policy configuration.

The Area selection tool filters the list of Areas according to the following criteria:

- by Area Name
- by Area Code
- by Area Type
- by Country
- by Organization

Req. 13. CARD uses the list of Areas and Area Types provided by CGD for data access policy configuration and evaluation (see section 6.2)

Req. 14. CARD provides a function to keep in sync the Area information used by the CARD.

5.9 Location

The term Location refers to a geographical location that is used to characterize some types of resources within the SSN Ecosystem. In the SSN Ecosystem, locations generally refer to ports.

The list of Locations is stored in the CLD. Each Location is identified by a unique code, named LOCODE, which is an extension of the UN/LOCODE Code List

5.9.1 Location attributes

Maximum number of Locations: 100.000

Attribute	Type	Description	Example
Location Code	String `"^[A-Z0-9]{2,20}$"`	The alphanumeric code of the location	“FRLEH”
Location Name	String	The name of the Location	“Le Havre”
Country **(optional)**	<Country_Code>	The Country which the Location is associated to	“FR”
Geographical Area **(optional)**	<Area_Code>	The Area associated with the Location	“GEO_123456”
Organization **(optional)**	List of <Organization_Code>	The Organization(s) which the Location is associated to	“ORG_FR123456”, “ORG_FR123457”

The CLD provides the following information by means of an export function:

- the list of Locations and their attributes.

CARD uses the information provided by the CLD to configure and evaluate the data access policies, whenever there is a reference to a Location.

The Bidder should propose a synchronization strategy on how the CARD retrieves and uses the CLD information taking into consideration the size and structure of the CLD database as well as the CARD availability and performance requirements. During the sync CARD checks if there are inconsistencies with the existing policies. In case of problems, the CARD Administrator is warned about the type of inconsistency and the sync procedure can be stopped.

5.9.2 Location Filter

CARD provides an “Location selection tool” that can be used by the CARD Administrator during the Policy configuration.

The Location selection tool filters the list of Locations according to the following criteria:

- by Location Name
- by Location Code
- by Country
- by Organization
- by Area

Req. 15. CARD uses the list of Locations provided by CLD for data access policy configuration and evaluation (see section 6.2)

Req. 16. CARD provides a function to keep in sync the Location information used by the CARD.

6 Data Access Policy Configuration

The CARD Administrator is responsible for the configuration of the data access policies. After a configuration effort during the initial deployment of CARD, the policy configuration activity should be occasional and limited to changes in the SSN Ecosystem that require the introduction of new profiles and roles or the update or removal of existing ones.

CARD reads the user account information to dynamically evaluate the applicable data access policies. Data access policies are defined based on the following four attributes of the user account: its Profiles, its Country, its Organisation, and the Operations associated to the account.

User’s Attribute	Cardinality	Example	Meaning	Usage
USER_PROFILE	None, one or more	CST, SAR	The high level role of the user within the SSN Ecosystem applications	Different Roles and data access policies are associated to different user’s Profiles

USER_COUNTRY	One	PT	The country or international institution which the user is associated to	Some data access policies depend on the user's Country, e.g.: access is limited to resources from the user's Country
USER_ORGANIZATION	One	ORG_PT12345	The organization (e.g. Italian Coast Guard) which the user is associated to.	Some data access policies depend on the user's Organization: e.g. access to a resource is granted only if its Location is under the jurisdiction of the user's Organization
USER_OPERATION	None, one or more	SAFEMED	The Operation the user is part of (Operations are used to tag information items and limit their access).	Some data access policies grant access to a resource only if the user is part of the specific Operation.

The Profiles define the Roles, and thus the Resources, that the user account has access to, and the data access limitations applied to each role. The Country, the Organization and the Operations may be used to configure the access limitations.

Figure 5 shows the relations between User, Profiles, Roles and Limitations. Note that the user account details and the Profiles associated to the user account are stored in the IdM, the system responsible for the user management. On the other hand the data access policy (relationship between Profiles, Roles and Limitations) are stored in the CARD.

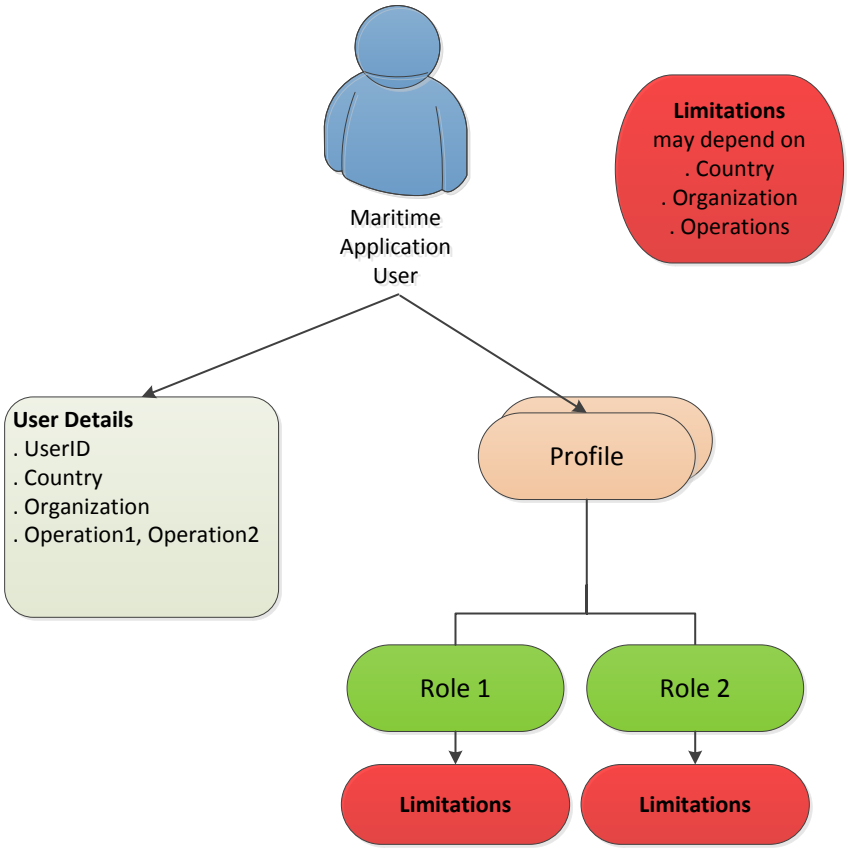


Figure 5 – User, Profiles, Roles and Limitations

6.1 Policy Configuration workflow

The configuration of a data access policy starts by selecting a Profile from the list of available Profiles.

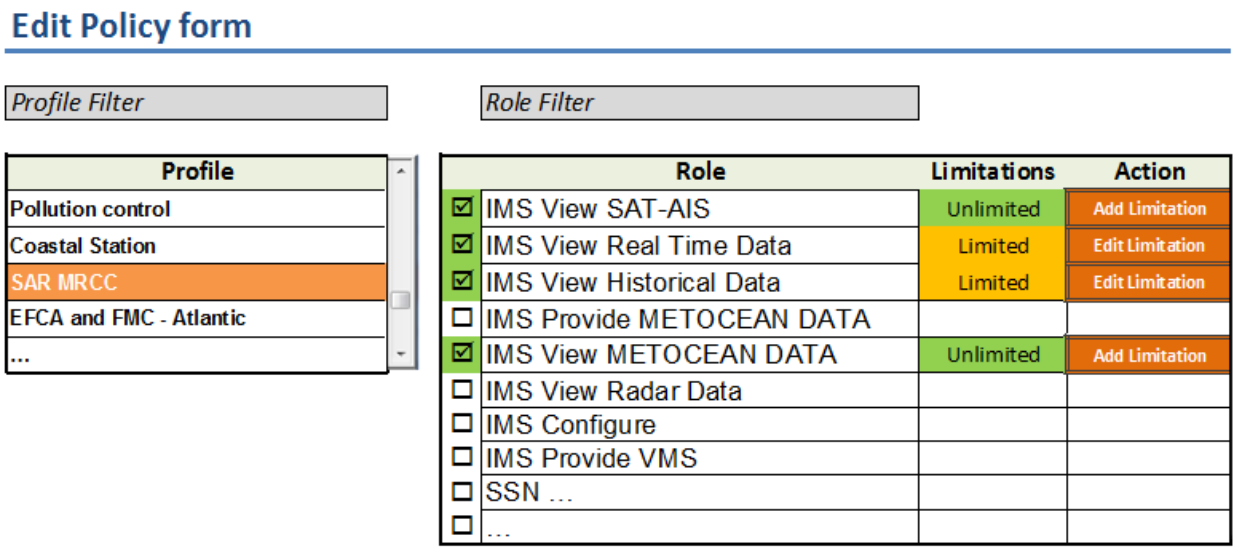
Once the Profile is selected, the CARD Administrator associates one or more Roles to the selected Profile.

For each Role that is selected, by default the CARD provides unlimited access to the underlying Resource. The CARD Administrator may then define one or several Limitations on this Role.

If a Role has already limited access, the CARD Administrator may edit the Limitation(s).

For configuration of Limitations see section 6.2.

6.1.1 Edit Policy form (mock-up)



6.2 Limitations

When a data access policy is created for a given Profile, access to a resource may be restricted. A Limitation defines the level of restriction applied by the policy. If a policy contains a Limitation then the Limitation can be one of the following types.

Limitation Type	Description	Example
Full Access	User can access the resource with no limitation. This is the default approach.	User has unlimited access to METOCEAN data
Source	The access is restricted to data provided by: - Selected group of countries, or - The user's country.	Data source is a Country that belongs to the EU EFTA group of countries
Location	The access is restricted to resources associated to Locations within: - Selected group of countries, - The user's country, or - The user's organization.	Access limited to Port Calls of ships bound to the user's Country
Area	The access is restricted to resources which coordinates are within: - Selected geographical areas, - Areas of selected types covered by the user's country, or - Areas of selected types covered by the user's organisation.	Access limited to ship positions in the Baltic Sea
Operation	The access is restricted to data related to the selected operation(s).	Access limited to the SAFEMED resources
Data Type	The access is restricted to data of: - Specific types. - Types depending on user's organization, or - Types depending on the user's country.	Access limited to Incident Reports of type "POLREP".

The different types of limitations that can be applied to a resource are described in the following sections.

6.2.1 Selections Criteria for Limitations

In order to describe in an easier way the different kinds of limitations the following selection criteria are defined. There are 4 types of selection criteria: Country, Location, Geographical Area and Data Types.

Important Note: the combination of selection criteria of the same type is made by using a logic OR.

6.2.1.1 COUNTRY_SELECTION_CRITERIA

CARD selects one or more countries/institutions from the CCD with one of these conditions or a combination (logic OR) of these conditions, called COUNTRY_SELECTION_CRITERIA:

1. identified by one or more CCD codes, e.g. “DE”
2. having a specific Country Type as defined in the CCD, e.g. “EFTA”
3. having a specific Regional Agreement as defined in the CCD, e.g. “Black Sea Commission”
4. The user’s Country (dynamically set by CARD based on the user’s details)

Examples (SQL-like notation)

```
select country_code from CCD where...
```

Sample Condition#	Type (static/dynamic)	Condition
Condition #1	static	`country_code in ('DE', 'IT')`
Condition #2	dynamic	`country_code = USER_COUNTRY`
Condition #3	static	`country_type = 'EFTA'`
Condition #4	static	`country_reg_agreement = 'Black Sea Commission'`

6.2.1.2 LOCATION_SELECTION_CRITERIA

CARD selects one or more Locations from the CLD with one of these conditions or a combination (logic OR) of these conditions:

1. identified by a list of Location codes, e.g. (“ESCAD”, “FRLEH”)
2. belonging to a specific group of Countries, as defined in the CLD
3. belonging to a specific Organization or its children Organizations in the hierarchy, as defined in the COD

4. belonging to the user's Country (dynamically set by CARD based on the user's details), as defined in the CLD

5. belonging to the user's Organization (dynamically set by CARD based on the user's details), as defined in the COD

The list of Locations associated to a Country or Organization is fixed, regardless of the Profile or Role.

Examples (SQL-like notation)

```
select locode from CLD where...
```

Sample Condition#	**Type (static/dynamic)**	**Condition**
Condition #1	static	`locode in ('ESCAD', 'FRLEH')`
Condition #2	static or dynamic	`locode_country in COUNTRY_SELECTION_CRITERIA` (see section 6.2.1.1)
Condition #3	dynamic	`locode_organization in USER_ORGANIZATION`

6.2.1.3 AREA_SELECTION_CRITERIA

CARD selects one or more geographical areas from the CGD with one of these conditions or a combination (logic OR) of these conditions:

1. identified by a list of CGD codes, e.g. "A123456"

2. having a specific Area Type, as defined in the CGD, e.g. "TSS"

3. belonging to a specific Country AND with a specific Area Type, as defined in the CGD

4. belonging to a specific Organization AND with a specific Area Type, as defined in the COD

5. belonging to the user's Country AND with a specific Area Type, as defined in the CGD

6. belonging to the user's Organization (or children Organizations) AND with a specific Area Type, as defined in the COD

The geographical areas with a specific Area Type and associated to a Country/Organization are fixed, regardless of the Profile or Role.

Examples (SQL-like notation)

```
select area from CGD where...
```

Sample Condition#	**Type**	**Condition**

	(static/dynamic)	
Condition #1	static	`area_code in ('A1234567', 'A1234568')`
Condition #2	static or dynamic	`area_country in COUNTRY_SELECTION_CRITERIA` (see section 6.2.1.1)
Condition #3	dynamic	`area_country = USER_COUNTRY and area_type = 'EEZ'`
Condition #4	dynamic	`area_organization = USER_ORGANIZATION and area_type = 'PORT_AREA'`

6.2.1.4 DATA_TYPE_SELECTION_CRITERIA

CARD selects one or more Data Types with one of these conditions or a combination (logic OR) of these conditions:

1. associated to a specific Country, as defined in CARD
2. associated to a specific Organization, as defined in CARD
3. associated to the user's Country, as defined in CARD
4. associated to the user's Organization, as defined in CARD

Note that the associations of Country/Data Type and Organization/Data Type are defined in CARD since there is no equivalent of a "Central Database" for Data Types.

Examples (SQL-like notation)

```
select data_type from CARD where...
```

Sample Condition#	Type (static/dynamic)	Condition
Condition #1	dynamic	`data_type_country = USER_COUNTRY`
Condition #2	dynamic	`data_type_organization = USER_ORGANIZATION`

6.2.2 Full Access (No Limitation)

Depends on: User's **Profile**

A limitation of type “Full Access” allows in any case the use of the resource by the user with a specific Profile. Any request of permission to access the resource by such a user is granted.

6.2.3 Limitation based on Source

Depends on: selected group of **Countries**, User’s **Profile** and User’s **Country.**

A limitation of type “Source” refers to the provider of the resource.

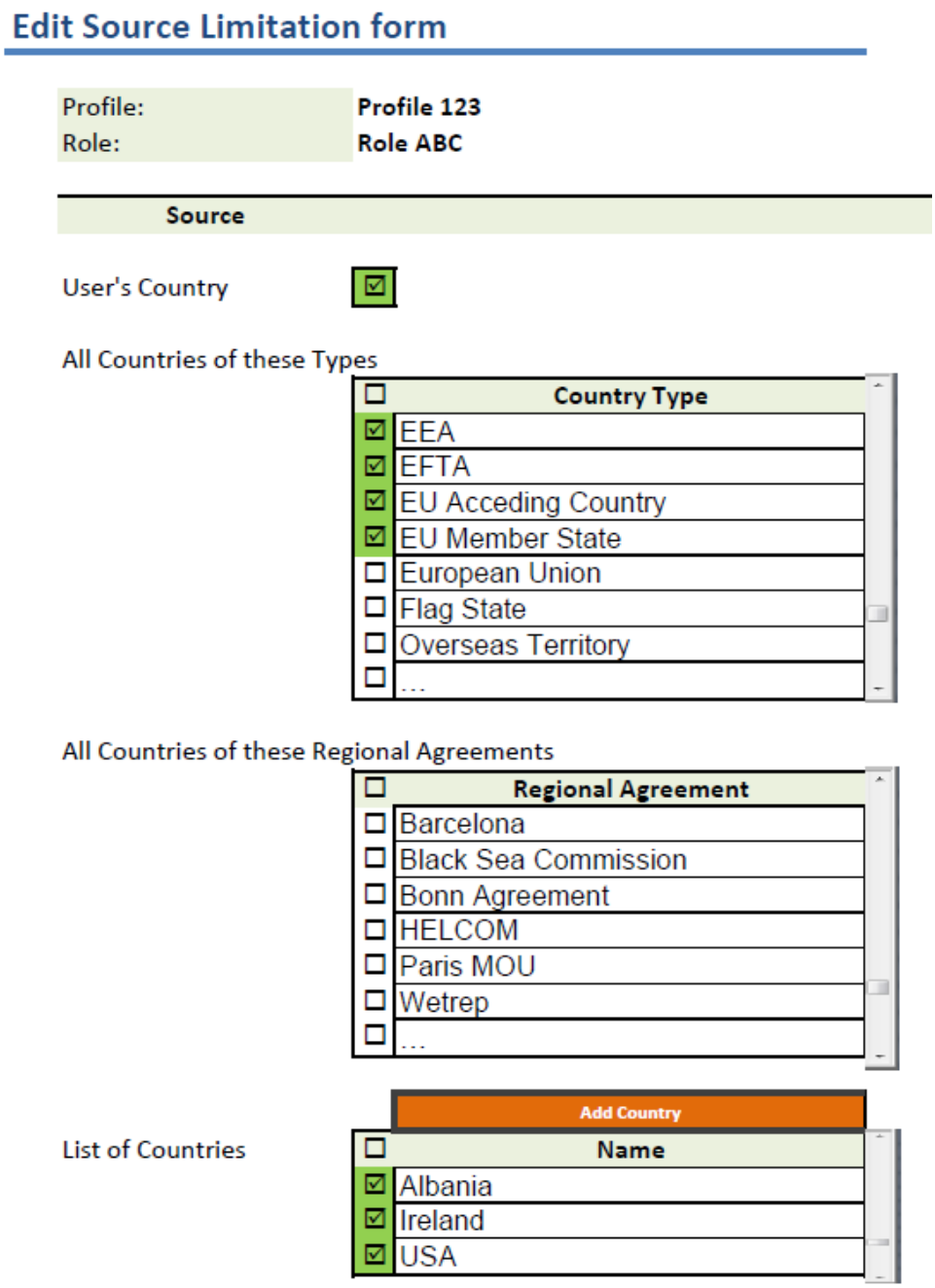
A limitation Source restricts the access to resources provided by one or more Sources that belong to a group of **Countries** selected using a specific COUNTRY_SELECTION_CRITERIA, as defined in section 6.2.1.1. In the reference access matrix (Appendix E to the Tender Specifications) the limitation Source is also indicated by the letter “S”, e.g. “S: EFTA” means that access is limited to the resources provided by the EFTA Countries.

Some examples of Source limitations are:

Profile	Coastal Station
Role	IMS View Pleasure Boat Data
Limitation	Type: Source `country_code = USER_COUNTRY`

Profile	PSC
Role	SSN View Voyage Waste
Limitation	Type: Source `country_type = ‘EU EFTA’`

6.2.3.1 Edit Source Limitation form (mock-up)



6.2.4 Limitation based on Location

Depends on: selected group of **Locations** or **Countries**, User's **Profile**, User's **Country** and User's **Organization.**

A limitation of type "Location" refers to the Location attribute of the resource (identified by a Location Code).

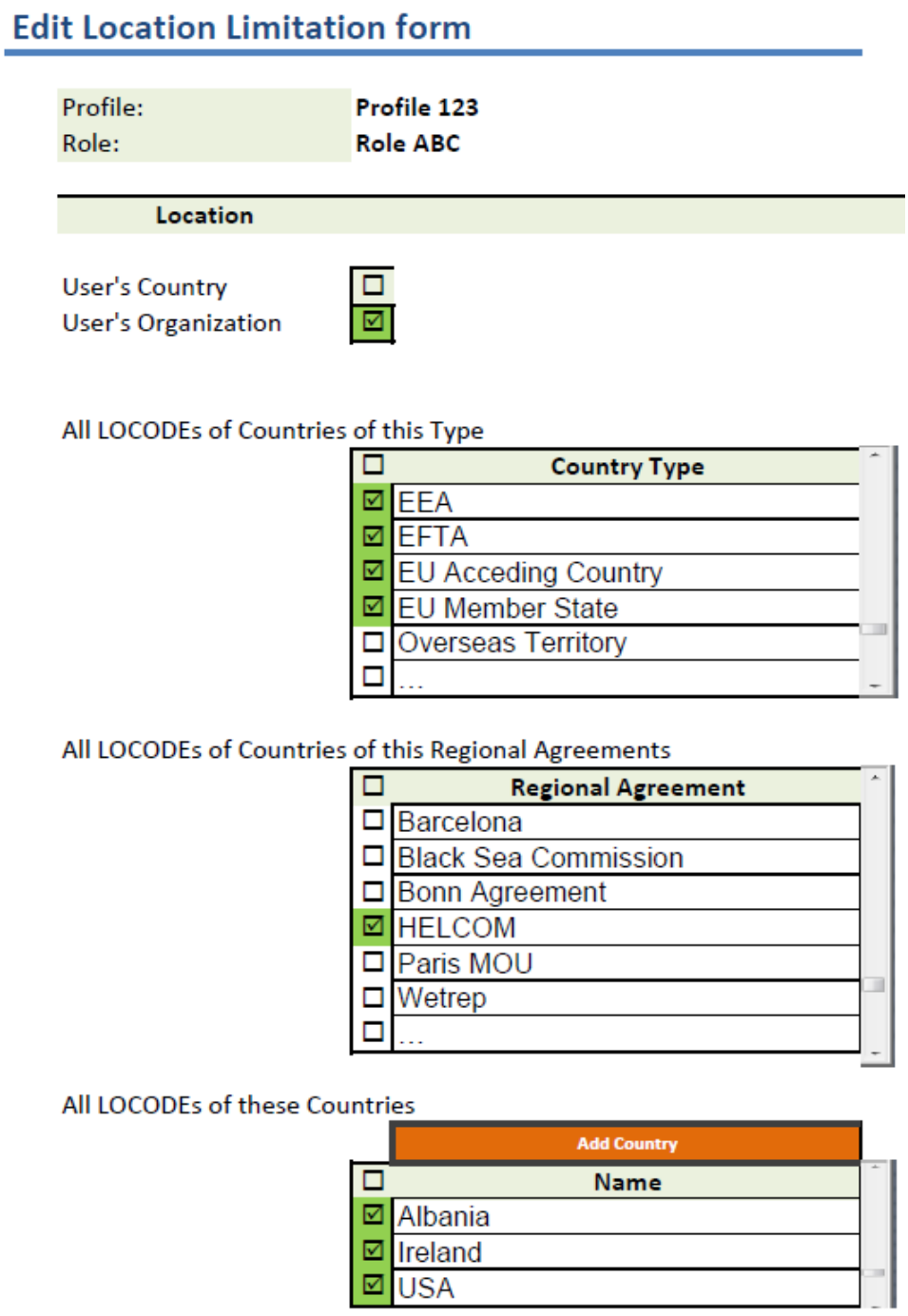
A limitation Location restricts the access to resources having an attribute Location that belongs to a group of **Locations** selected using a specific LOCATION_SELECTION_CRITERIA, as defined in section 6.2.1.2. In the reference access matrix (Appendix E to the Tender Specifications) the limitation Location is also indicated by the letter "L", e.g. "L: User's Organization" means that the access is limited to one of the Locations under jurisdiction of the user's Organization.

Some examples of Location limitation are:

Profile	Coastal Station
Role	SSN Provide Port Call
Limitation	Type: Location `locode_country = USER_COUNTRY`

Profile	PSC
Role	SSN View Exemptions
Limitation	Type: Location `locode_organization = USER_ORGANIZATION`

6.2.4.1 Edit Location Limitation form (mock-up)



6.2.5 Limitation based on Area

Depends on: selected group of **Areas**, User's **Profile**, User's **Country/Institution** and User's **Organization.**

A limitation of type "Area" refers to the geolocation (position defined by geographical coordinates) of the resource.

A limitation Area restricts the access to resources having their position within a polygon of a set of geographical areas from the CGD, selected using a specific AREA_SELECTION_CRITERIA, as defined in section 6.2.1.3. In the reference access matrix (Appendix E to the Tender Specifications) the limitation Area is also indicated by the letter "A", e.g. "A: BALTIC_SEA" means that access is limited to the Area named "BALTIC_SEA".

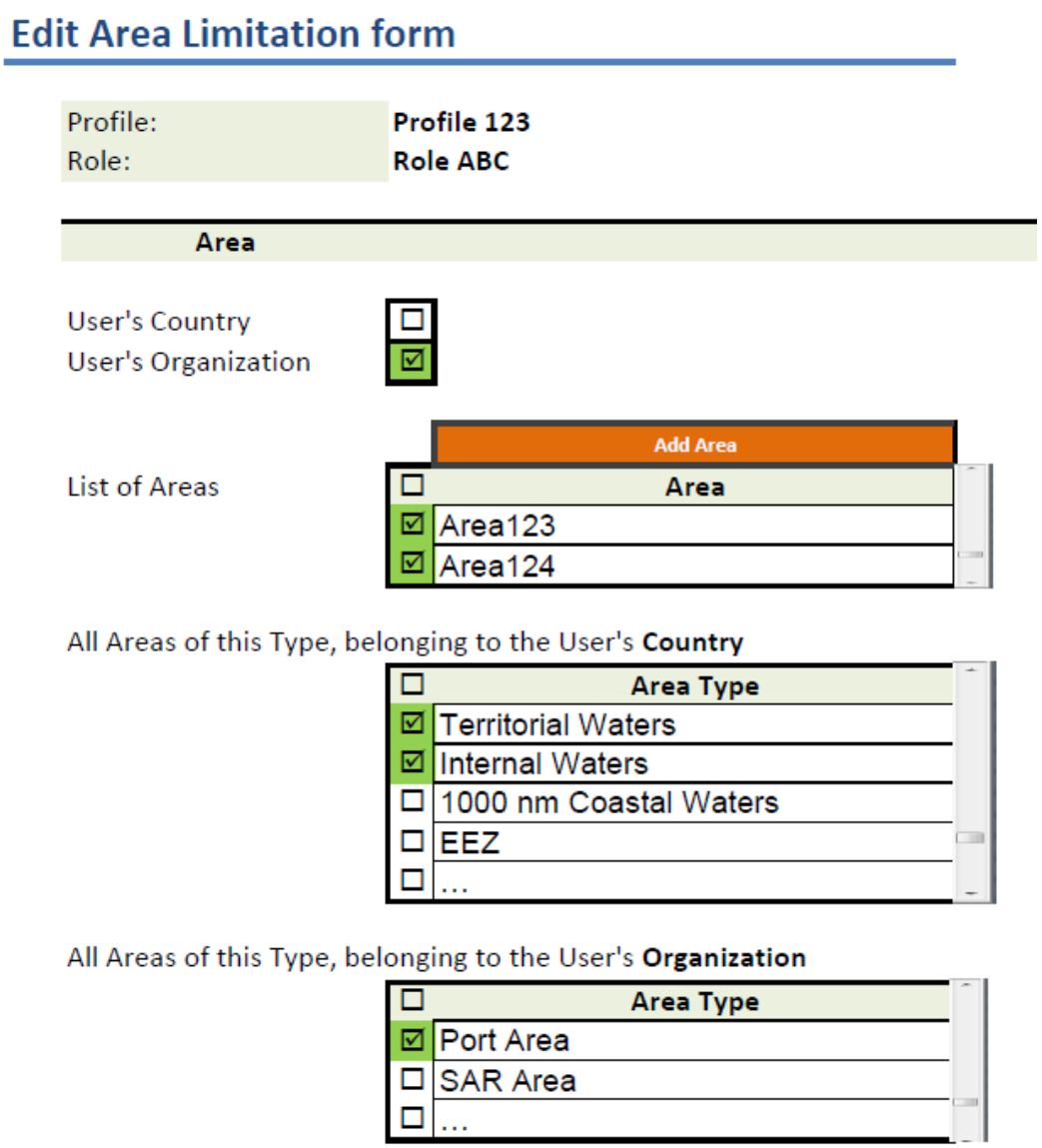
Some examples of Area limitation are:

Profile	Coastal Station
Role	SSN Receive Enriched AIS

Limitation	Type: Area
	`area_country = USER_COUNTRY`
	`area_type = 'COASTAL_AREA'`

Profile	EFCA and FMC Mediterranean
Role	IMS View VMS
Limitation	Type: Area `area_code = 'AREA_EFCA_MED'`

6.2.5.1 Edit Area Limitation form (mock-up)



6.2.6 Limitation based on Operation

Depends on: User's **Profile** and User's **Operation(s).**

A limitation of type "Operation" refers to the operation attribute of a resource. An operation is an activity during which some resources, e.g. data, are made available only to a specific user community.

A limitation Operation restricts the access to resources which attribute **operation** has a specific value (a string). In the reference access matrix (Appendix E to the Tender Specifications) the limitation Operation is also indicated by the letter "O", e.g. "O: SAFEMED" means that the access is limited to the resources of the Operation SAFEMED.

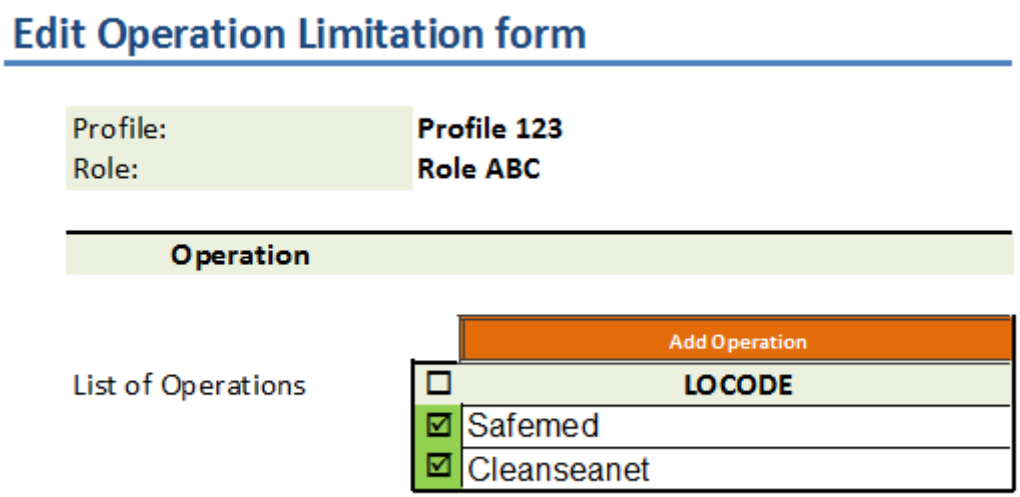
An example of Operation limitation is:

Profile	SAFEMED CSN

Role	EOS View EO image
Limitation	Type: Operation `operation = 'SAFEMED'`

Important Note: if a Profile is associated to a Role and the Role has the attribute resourceHasOperations set to TRUE then CARD assumes per default that there is no limitation based on the Operation. CARD therefore grants access to all Operations unless the CARD Administrator changes the configuration.

6.2.6.1 Edit Operation Limitation form (mock-up)



6.2.7 Limitation based on Data Type

Depends on: selected **Data Types**, User's **Profile**, User's **Country/Institution** and User's **Organization.**

A limitation of type "Data Type" refers to the **type** attribute of a resource.

A limitation "Data Type" restricts the access to resources which attribute **type** has a specific value or is in a list of values, as defined in section 6.2.1.4. In the reference access matrix (Appendix E to the Tender Specifications) the limitation Area is also indicated by the letter "T", e.g. "T: User's Organization" means that the access is limited to the resources with one of the Data Types associated to the User's Organization.

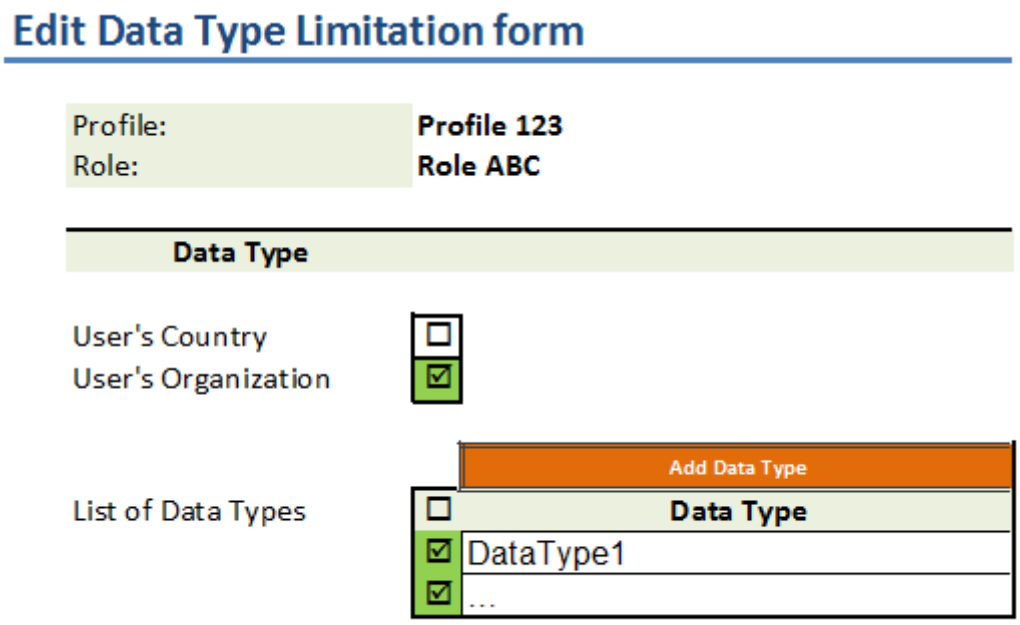
An example of Data Type limitation is:

Profile	PSC
Role	SSN Provide Incident Report

Limitation	Type: Data Type All Data Types associated to the user's Organization

Important Note: if a Profile gives access to a Role and the Role has the attribute resourceHasDataTypes set to TRUE then CARD assumes per default that there is no limitation based on Data Type. CARD therefore grants access to all Data Types unless the CARD Administrator changes the configuration.

6.2.7.1 Edit Data Type Limitation form (mock-up)



Req. 17. CARD provides all the necessary tools to configure and maintain the Data Access Policy Limitations.

7 CARD Administration Tools

This chapter describes the tools that support the administration of CARD.

7.1 Profile Management

In order to assist the CARD Administrator with the policy configuration tasks, in addition to the tools described in the previous chapters, CARD provides the following functions.

1. **Delete Profile**: delete a Profile and the associated data access policy. The action requires an explicit confirmation by the CARD Administrator.

2. **Clone Profile**: create a new Profile and configure the data access policy by copying the one associated to another Profile that has already been created.

3. **Import/Export of the CARD Configuration file**: download a file that contains the configuration of one or more selected items (Profiles, Roles, Countries, Organizations, etc.) and associated data access policies stored in the CARD, e.g. in XML format; the file is editable by the CARD Administrator using a standard text editor; the file can be uploaded and the CARD Configuration should be changed according to its content. This tool is particularly important during testing and deployment of CARD in different Environments, e.g. exporting the CARD Configuration file in Pre-Production and importing the file in Production.

4. **Bulk Policy Update**: update one or more Profiles by applying the same change at once, e.g. add/remove access to a Role or a group of Roles, or set some limitation for a selected group of Profiles and Roles. The action requires an explicit confirmation by the CARD Administrator.

5. **Bulk Country/Organization Update**: update one or more Countries and/or Organizations by applying the same change at once, e.g. add/remove access to a group of Data Types or Profiles. The action requires an explicit confirmation by the CARD Administrator.

The Bidder should propose more tools that can improve the efficiency of the CARD Profile management.

7.2 Backup

CARD provides a backup function that makes it possible to save a safety copy of all the CARD data and settings (reference data, policies, log files, etc.). A corresponding restore function reads the backup file and restores the CARD status at the moment of the backup.

Req. 18. CARD provides tools and functions to assist the administration and data access policy configuration tasks.

Req. 19. CARD provides a backup/restore function to save and recover a backup file of the CARD data and settings.

8 User Interface

The CARD user interface is web based and integrated with the existing EMSA Liferay portal technology (see section 10 and following sections).

The CARD data display and update forms are simple, intuitive and responsive (the average response delay of any action should be less than 1 sec; the maximum response delay should be less than 5 sec).

When saving the changes, the CARD Administrator should always be asked for confirmation and informed about the progress and status of the procedure.

8.1 Tabular Data

The lists of information items are displayed in tabular format.

The sequence of the records in the tables can be order by any of the table columns, in ascending or descending order.

The items displayed in a table can be filtered by substring. If the user sets a filter in a specific column, the table only shows those lines that contain the substring. The user can set filters on several columns. CARD combines the filters (logical AND) and shows the result.

Tabular data can be exported in CSV (UTF-8 character encoding) and Microsoft Excel 2010 format.

Tabular data can be imported in CSV (UTF-8 character encoding) format, if an import function is available.

Req. 20. CARD provides a web based user interface integrated in the existing EMSA environment, responsive and easy to use.

Req. 21. CARD provides sorting, filtering and export function for tabular data.

9 Data Access Policy Enforcement

CARD is the repository for the Data Access Policies of the SSN Ecosystem. CARD does not actually enforce a policy since the access to the resources is technically provided by the Maritime Applications.

CARD however provides all the information necessary for a Maritime Application to enforce the Data Access Policies by:

a) Distributing the definition of all policies and reference data stored in the CARD (“Policy Distribution service”), and

b) Making available a Data Access Authorization Service.

It is recommended that the Maritime Applications take advantage of the CARD Data Access Authorization service (point “b” above) whenever there is a need to grant or deny access to some resources. In some cases however the Maritime Application may download a read-only copy of the Policy definition by means of the Policy Distribution Service (point “a” above) and directly authorize (or not) the access to the resources.

The IdM uses the Policy Distribution Service to keep in sync all the information that is needed during the creation and update of users.

The use of the Policy Distribution Service may also be necessary in case of very high performance requirements that cannot be met by CARD or complex data access limitations that are not implemented by CARD.

9.1 Data Access Policy Version

In order to support the enforcement process, CARD provides a mechanism to combine several updates into a single new version of the CARD Data Access Policy. The CARD Administrator can therefore perform several changes in the configuration of the CARD and then publish the new version of the Data Access Policy in a single shot.

Every time the CARD Administrator publishes a new version of CARD Data Access Policy, CARD issues a new **Policy Version Number** (a sequential integer) that, if needed, can be retrieved by the Maritime Applications in order to compare the version of the Policy currently stored locally in their databases with the version published by CARD.

9.2 Enforcement Rules

CARD requires some rules in order to correctly enforce the data access policies as they are defined by the CARD Administrator.

9.2.1 Combination of Profiles

If a user has several Profiles, CARD combines the policies associated with each Profile using a logical 'OR', i.e. the fact of **having more than one Profile extends the access rights of a user**.

As an example, if a user has the following Profiles:

- Profile "Port" (which grants access to the Role "Provide Port Call"), and
- Profile "SAR MRCC" (which grants access to the Role "LRIT SAR SURPIC"),

then the user will be granted access to both Roles "Provide Port Call" and "LRIT SAR SURPIC".

9.2.2 Combination of Limitations for a single Profile

If in the policy associated to the user's Profile the access to a Role is limited by several Limitations of different kind (S, L, A, T, or O), CARD combines the Limitations by means of a logical 'AND', i.e. the fact of **having more than one Limitation further reduces the access rights of a user**.

As an example, if a user has the hypothetical Profile "Port" that sets the following Limitations on the Role "View T-AIS data":

- Limitation: Source = "Italy" (which restricts access to T-AIS data provided by Italy), and
- Limitation: Area = "Adriatic Sea" (which restricts access to T-AIS data in the Adriatic Sea),

then CARD will allow access only to T-AIS data provided by Italy and only if the position coordinates are within the Adriatic Sea area.

9.2.3 Combination of Limitations for several Profiles

If a user has several Profiles and in these Profiles there are limitations on the same Role, CARD first applies the limitations of each Profile separately (see the previous sections above) and then combines the resulting grant decisions by means of a logical 'OR'.

As an example, if a user has the following Profiles and Limitations on the Role "View T-AIS data":

- Profile "Port"
    - Limitation: Area = "User's Organization" (i.e. access to T-AIS data is limited to the area of jurisdiction of the user's Port)
- Profile "Coastal Station"
    - Limitation: Source = "User's Country" (i.e. access to T-AIS data is limited to positions provided by the user's Country)

then CARD will grant access to T-AIS data for the Port area, regardless of the source, plus to any T-AIS provided by the user's Country, regardless of the coordinates.

Req. 22. CARD implements the rules that combine the Data Access Policies when the user has several Profiles and/or there are several limitations on the same Role as described in section 9.2.

9.3 Policy Distribution Service

CARD provides a service that distributes on request the Data Access Policies definitions and reference data to Maritime Applications. By means of this service the Maritime Applications can keep a local read-only copy of the policies if deemed necessary for reliability and performance purposes.

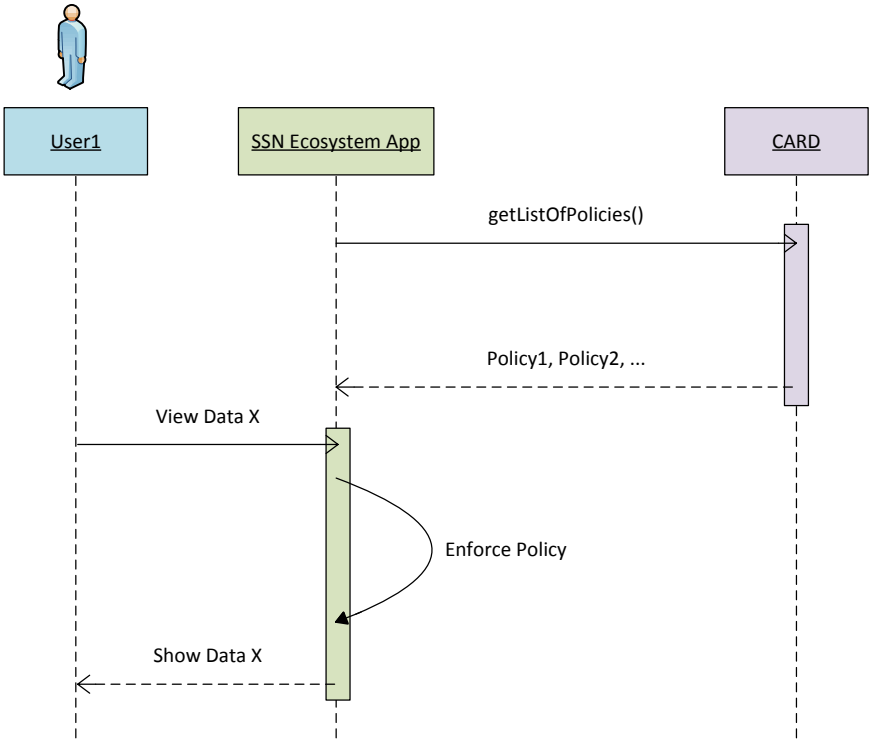


Figure 6 - Policy Distribution Service (sequence diagram)

The distribution is done by means of a Web Service, as a minimum. In addition to the Web Service, the distribution may also be done by means of a different protocol to be described by the Bidder. In any case, the communication protocol should implement existing industry standards, if available.

Important Note: in order to support the Data Access Policy synchronization process, data records returned by the Policy Distribution Service must have a specific field identifying the date and time (UTC) of the last change. Additionally, an external system can request all items that have changed since a specific date and time.

The distribution service includes as a minimum the following requests (or equivalent):

Request	**See section**
1. getListOfServices(): CARD provides the full list of Services including all attributes	5.1
2. getListOfRoles(): CARD provides the full list of Roles including all attributes	5.4
3. getListOfRoles(Service): CARD provides the full list of Roles including all attributes that are associated to the given Service	5.4

4. getListOfRoles(Profile): CARD provides the list of Roles associated to the given Profile, regardless of the limitations	5.4
5. getListOfDataTypes():CARD provides the full list of Data Types including the corresponding Role and all other attributes	5.7
6. getListOfDataTypes(Role):CARD provides the full list of Data Types for the given Role including all attributes	5.7
7. getDataTypes(Country or Organization): CARD provides the list of Data Types associated to the given Country or Organization	5.7
8. getListOfOperations():CARD provides the full list of Operations	5.3
9. getListOfOperations(Role):CARD provides the list of Operations for the given Role	5.3
10. getListOfProfiles(): CARD provides the full list of Profiles	5.2
11. getListOfProfiles(Service): CARD provides the list of Profiles having Roles associated to the given Service	5.2
12. getListOfProfiles(Organization): CARD provides the list of Profiles associated to the given Organization	5.6
13. getListOfPolicies(): CARD provides the full list of Policies, one Policy for each Profile, including all granted Roles and any Limitation	6.2
14. getPolicy(Profile): CARD provides the Policy for the given Profile, including all granted Roles and any Limitation	6.2
15. getLimitations(Profile, Role): CARD provides the Limitations for the given role and Profile	6.2
16. getListOfPolicies(User): CARD provides the full list of Policies, one Policy for each Profile, including all granted Roles and any Limitation evaluated for the given user	6.2
17. getPolicy(Profile, User): CARD provides the Policy for the given Profile, including all granted Roles and any Limitation evaluated for the given User	6.2

18. getLimitations(Profile, Role, User): CARD provides the Limitations for the given Profile, Role and evaluated for the given User	6.2
19. getPolicyVersionNumber(): CARD provides the version number of the Data Access Policy currently published by the CARD Administrator.	9.1

Req. 23. CARD provides a Policy Distribution Service as described in section 9.3.

9.4 Authorization Service

CARD provides a service that, for a given user, grants or denies access to a resource, identified by a Role. This is in fact an implementation of the policies stored in CARD itself, in a way that the Maritime Application fully relies on CARD for policy enforcement and for taking a decision on granting, or not, access to a resource (see Figure 7).

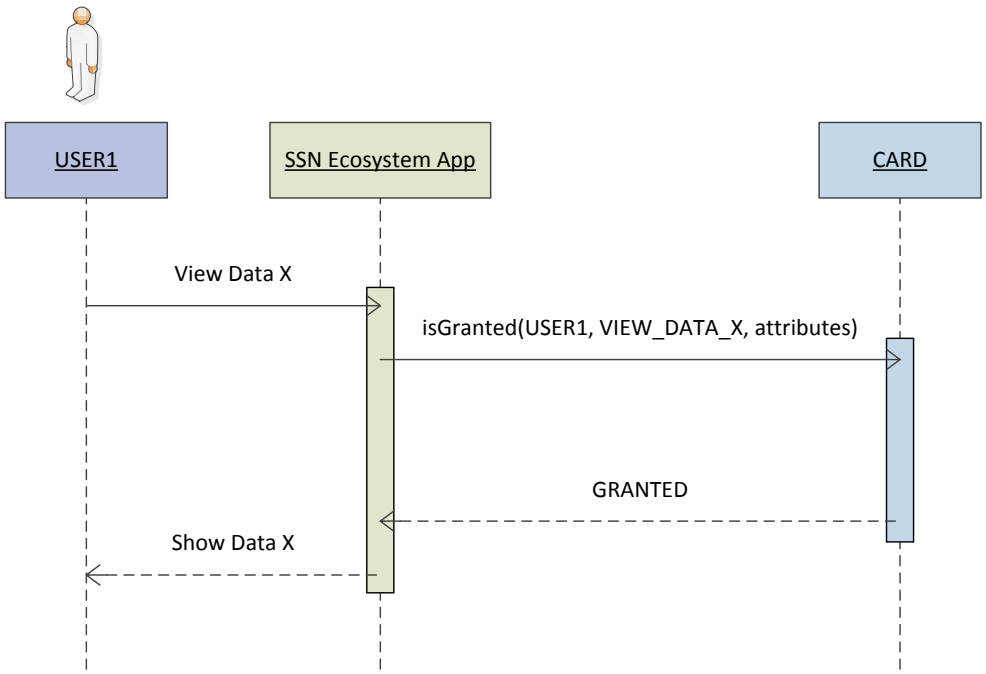


Figure 7 - CARD Authorization Service (sequence diagram)

The Authorization Service is done, as a minimum, in two ways by means of:

- a Web Service
- a service that is compatible with the Java Authentication and Authorization Service (JAAS)

In addition, the Authorization may also be done by means of a different protocol to be described by the Bidder. In any case, the communication protocol should implement existing industry standards, if available.

The Authorization Service includes the following requests (or equivalent):

- isGranted(User, Role): CARD responds with

- GRANTED, if the user is granted access to the *simple resource* identified by the Role (see section 5.4)
- DENIED, if the user is denied access to the *simple resource* identified by the Role (see section 5.4)
- ERROR, if the User or the Role do not exist or if the Role refers to a complex resource (see section 5.4); error message explaining the nature of the exception, e.g. “Role refers to a complex resource, resource attributes are required to evaluate the data access policy”.

- isGranted(User, Role, resourceAttributes): CARD responds with
  - GRANTED, if the user is granted access to the resource identified by the Role and having the given attributes; resourceAttributes is a list of (key, value) pairs describing the specific resource that is being accessed according to 5.4.2.
  - DENIED, if the user is denied access.
  - ERROR, if the user or the role does not exist or the request parameters are not valid; error message explaining the nature of the exception.

  Example:

```
isGranted(“USER123”,
          “PROVIDE_INCIDENT”,
          “{source=FR, location=FRLEH, data-type=PROVIDE_INCIDENT.BANNED}”)
```

CARD retrieves the user Profile(s) and evaluates all the data access policies associated to the given Role.

If the data access policy has any limitation, CARD evaluates the limitation by setting, if applicable, the dynamic criteria (USER_COUNTRY, USER_ORGANIZATION, USER_OPERATION) and retrieving the corresponding information from the Central Databases and/or the local CARD database.

9.4.1 Enforcement of Area Limitation

In case of an Area Limitation, the CARD Authorization Service supports as a minimum areas of category “Bounding Box” (max. latitude/longitude, min. latitude/longitude). The information on the Area Category is provided by the CGD.

The Bidder should indicate in their bid if their solution also works, i.e. meets the functional and performance requirements, with different area categories, for instance “Polygon” or “Circle”.

9.4.2 Simulator

CARD provides a “Simulator” tool that shows the result of a simulated authorization request for a real user submitted by the CARD Administrator to the Authorization Service. The Simulator explains which rules and limitations were applied in order to obtain the grant or deny decision.

Req. 24. CARD provides an Authorization Service that supports different protocols as described in section 9.4; CARD provides a Simulator of the Authorization process.

9.5 Reference Scenarios

The Reference Scenarios described in this section are used to validate the proposed solution.

9.5.1 Reference Scenario A

“Service A” is a web-based applications that is using a basic Role-Based Access Control method to grant or deny users access to some resources. The grant/deny decision is binary and no further restrictions are applied in case of a “grant” (no limitations).

“Service A” has a total of 500 users, grouped in 5 roles, for a total of 50 resources be protected (e.g. web pages). The average number of concurrent open sessions is 100 and a web page should be loaded in 0.5 s. “Service A” is using a JAAS solution to implement the authorization mechanism.

The Bidder should describe how the “Service A” will be integrated into the proposed solution of CARD, the necessary changes (if any) on the “Service A” application and the configuration effort.

9.5.2 Reference Scenario B

“Service B” is a ship position message processing module that receives an input stream of AIS data. For every position message “Service B” checks if a subscribed user is authorized to access the data or not. If the user is authorized, the position message is forwarded to the user.

The authorization decision is based on the following rule:

- user has the role “View AIS”
- user’s country belongs to “Country Group AIS” (S: “AIS_COUNTRY”)
- the position is within the coastal polygon of the user’s Country (A: User’s Country/COASTAL_AREA)

There are 50 possible roles, 100 users are subscribed to “Service B” and the rate of positions is 50 message/s. “Service B” is using an Oracle Entitlement Server solution to implement the authorization mechanism.

The Bidder should describe how the “Service B” will be integrated into the proposed solution of CARD, the necessary changes (if any) on the “Service B” application and the configuration effort.

9.5.3 Reference Scenario C

“Service C” is a Web Map Service (OGC –WMS version 1.3.0). For every WMS-GetMap request the “Service C” should check if a subscribed user is authorized to access the image or not. If the user is authorized, the image is forwarded to the user.

The authorization decision is based on the following rule:

- user has the role “View Map”
- the layer (Data Type) specified in the GetMap request is authorized for the user (T: Layer1)
- the area (Bounding Box) specified in the GetMap request is within the Area limitation (A: AREA1)

There are 50 possible roles, 100 users are subscribed to “Service C” and the rate of GetMap WMS requests is 1 request/s. “Service C” has currently no authorization mechanism in place and it should preferably rely as much as possible on the CARD Authorization Service with no significant changes on the “Service C” application.

The Bidder should describe how the “Service C” will be integrated into the proposed solution of CARD, the necessary changes (if any) on the “Service C” application and the configuration effort.

Req. 25.	The Bidder shall describe how the proposed solution addresses the Reference Scenarios.

10 Technical architecture

CARD and its functions are highly critical to all EMSA applications. Not having CARD available might cause a complete downtime of most applications, preventing EMSA to perform contractual and legal obligations to organizations and Member States.

It is therefore a Mission Critical system and shall be designed as such..

Taking into consideration the high level of criticality, CARD shall respect the following design requirements:

1. CARD shall not have or be a single point of failure.
2. CARD components shall use active-active clustering techniques to ensure availability and resilience.
3. CARD shall be designed to have a fully redundant infrastructure and software architecture.
4. Basic and minimum requirements for the redundant infrastructure:
    a. Cluster with 2 nodes (non-functional tests might show the need to split components into different clusters);
    b. Integration Tier to be implemented in the existent OSB infrastructure (see the annex “EMSA System and Application Technical Landscape” for details);
    c. Database schemas to be deployed in the existent DB RAC (see the annex “EMSA System and Application Technical Landscape” for details).
5. Basic and minimum requirements for the Software architecture:
    a. n-tier architecture: presentation, business, integration and data tiers to be considered as a design pattern
    b. JAAS (Java Authentication and Authorization Service) module compatible with EMSA technical landscape is mandatory for Weblogic and Tomcat.
    c. Caching mechanism to allow faster responses to requests
6. CARD components shall be compliant with the EMSA BCF strategy to ensure Business Continuity (see the annex “EMSA System and Application Technical Landscape” for details).

Most of the topics above are addressed in more details in section “12 - Non-Functional Requirements” below.

Within their bids, Bidders shall describe with as many details as possible, the foreseen CARD architecture in-line with the requirements presented in this document and taking into consideration all annexes provided in this tender.

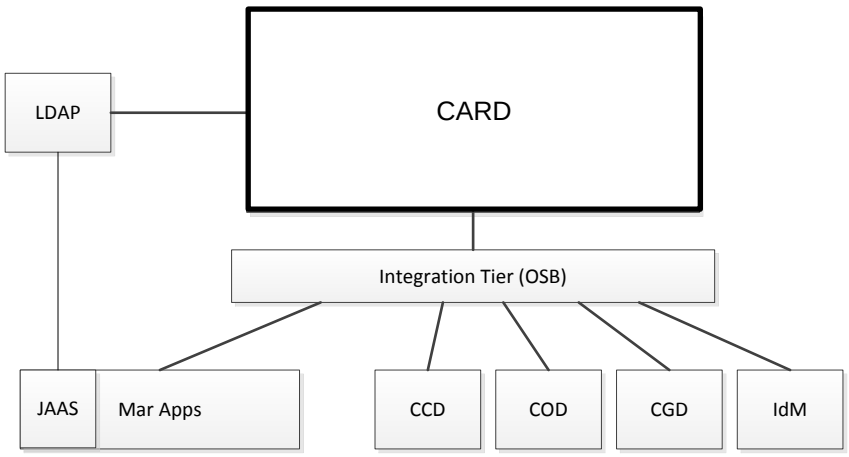
If any deviation is required, it must be fully identified in the bid, properly detailed and justified.

Req. 26.	CARD is compliant with the technical architecture described in section 10.

11 Technical Interfaces

This chapter describes how CARD retrieves the information from external systems (central databases).

The following figure shows the main expected interfaces:



- IdM will interface with CARD to:
    - Provision Users and their association with Profiles and Roles (creation and updates)
    - Obtain the full list of Profiles, Roles, corresponding attributes and their associations. For synchronization purposes every element must have a field identifying the date and time of the last change to the element.
- CARD will interface with the Common Databases to retrieve the base information used in CARD
- CARD will provide a realm module to allow JAAS to be used by the application server and by the maritime applications
- Integration tier.

11.1 Identity Management

The IdM, as introduced in section 3.2.1, provides the user's details that are taken into account by the CARD to evaluate the data access policies. CARD needs the user attributes defined in section 6.

The IdM provides the user's information to CARD by means of a service. CARD calls this service to retrieve the user details.

A preliminary technical documentation of IdM services is provided in Appendix D of the tender specifications for information. The updated set of documents will be made available to the winning tenderer at the date of signature of the contract.

11.2 Central Databases

The interfaces to the Central Databases used by the CARD are described in the following sections.

In order to ensure the availability and performance requirements, CARD provides a caching mechanism that is used in case the Central Databases are not available, i.e. a read only copy of the reference data. The Bidder should explain in their bid the proposed solution to address this synchronization need and the possible reduction of service in case of not availability of one or more Central Databases.

A preliminary technical documentation of the central databases services is provided in Appendix C of the tender specifications for information. The updated set of documents will be made available to the winning bidder at the date of signature of the contract.

11.2.1 Central Country Database (CCD)

The Central Country Database (CCD) provides the full list of Countries as an export file, in CSV format, as well as the reference data (Country Categories, Types, Regional Agreements).

Due to the very small number of changes in the CCD database, the synchronisation of the CCD information between CARD and CCD is initiated manually by the CARD Administrator. CARD imports the relevant CCD information from the CCD export file and stores it in a local table for data access policy configuration and evaluation purposes.

11.2.2 Central Organization Database (COD)

The Central Organization Database (COD) interface is a Web Service that provides on request the information on Organizations as well as the reference data (Organization Types, etc.). The COD also provides a subscription service that broadcasts an announcement when a new record in the COD database has been created or existing records have been changed or deleted.

CARD connects to the COD and retrieves the relevant Organization information whenever the information is needed for synchronization, data access policy configuration and evaluation purposes.

11.2.3 Central Location Database (CLD)

The Central Location Database (CLD) interface is a Web Service that provides on request the information on Locations.

CARD connects to the CLD and retrieves the relevant Location information whenever needed for synchronization, data access policy configuration and evaluation purposes.

11.2.4 Central Geo-reference Database (CGD)

The Central Geo-reference Database (CGD) interface is a WFS service that provides on request the information on Geographical Areas. CARD connects to the CGD and retrieves the relevant Area information whenever needed for data access policy configuration and evaluation purposes.

Req. 27. CARD implements the interfaces to the external systems and modules and provides the caching mechanisms that are necessary to its correct functioning.

12 Non-Functional Requirements

CARD is Mission Critical system; its criticality shall be considered for every non-functional design and architectural decision that has to be taken.

The high criticality shall drive the CARD design since the beginning, aiming the implementation of a system with high levels of availability, resilience and scalability.

12.1 Capacity and Data sizing

The following figures indicate the expected dimension of the SSN Ecosystem user community and the relevant authorization information:

Users: 10.000 (500 concurrent users)
Services: 50
Profiles: 200
Roles: 1.000
Organizations: 10.000

12.2 Scalability

Scalability can be defined as the ease with which a system or component can be modified to fit the new sizing needs.
CARD shall be able to easily “scale up” (adding more resources to an existent component) and “scale out” (adding new components to the infrastructure).

Within their bids, bidders shall describe as detailed as possible, how CARD will be able to “scale out”.

12.3 Resilience

Resilience can be defined as the capability of a system to remain stable under adverse conditions.
Being a highly critical component, CARD shall be designed and developed in such a way that:

- Shall be resilient enough to provide service with an acceptable level of deterioration in the following conditions:
  - Only with half of its established capacity, measured from an infrastructure point of view;
  - With a peak of load of the double of its nominal load.
- Business Continuity strategies can be implemented in-line with EMSA BCF strategy defined in “EMSA System and Application Landscape”;
- A Service Level Agreement can be clearly established and monitored;

Within their bids, bidders shall describe as detailed as possible how CARD will address Resilience and what are the expected impacts and deterioration in the service provided by CARD in the following two scenarios:

- **Only with half of its established capacity available;**
- **Receiving peaks of load of the double of its nominal load.**

12.4 Availability

The availability expectations of a system relate to how many hours in the day, days per week, and weeks per year the application is going to be available to its users and how quickly they should be able to recover from failures.

CARD is expected by the customer to be available 24 hours/day, 7 days a week. When systems do become mission critical and business needs warrant a very high availability, the system should be available 24 x 7 with an expected allowance of some minimal down time for regular maintenance.

The following overall availability requirements are defined for the CARD system:

- The expected availability is 24 x 7.
- The measured availability should be at least 99.9% per year.
- Recovery from any type of unplanned system outage should be successfully completed within 1 hour of the outage.
- The maximum downtime allowed during a week is two hours.

Within their bids, bidders shall describe as detailed as possible how CARD will address Availability and how it will react in the following two scenarios:

- **Planned maintenance intervention for deployment of a new version. Also provide a possible intervention plan;**
- **Unplanned maintenance intervention due to an infrastructure issue.**

12.5 Modularity and Reusability

The architecture of CARD shall be defined in such a way that modularity will be encouraged and promoted. This concept of modularity is applicable to both software designs and implementations and infrastructure design.

Promoting Modularity will also leverage Reusability.

The reuse philosophy should be applied in several areas:

- Design and develop using reusability is a key requirement.
- Reuse of existing commercial “off the shelf” hardware or software (COTS);

Within their bids, bidders shall describe as detailed as possible, how CARD will address Modularity and Reusability, what modules are foreseen to be reused (by whom), advantages and disadvantages found.

12.6 Performance Requirements

CARD shall support an expected load of 500 authorization requests per second in average.

The Bidder should indicate in their bid the nominal and maximum load that is supported by their solution.

12.7 Time Reference Requirements

CARD shall always use, store and provide date and time values in UTC, time zone **Z** (UTC±00:00).

Req. 28.	CARD meets all the non-functional requirements stated in the section 12.

13 CARD Administration and Activity Logging

CARD is administered by one or more members of EMSA staff having the following Profiles/Roles:

- **CARD Administrator**: responsible for the CARD system administration (management of Services, Roles Profiles, Data Types access to the Journal and other system administration tasks)
- **CARD Service Administrator**: responsible for the data access policy configuration, for the Roles that belong to his/her Service
- **CARD Viewer**: CARD is accessible in read-only mode by other EMSA Staff.

13.1 Journal

CARD logs all actions ("who did what and when") of the CARD Administrators whenever they update the CARD, by creating new items, or changing/deleting existing ones. The log information is stored in a repository that is called the CARD Journal. The Journal is accessible by the CARD Administration for routine usage monitoring and in case of an audit.

13.2 Automatic Activity Monitoring

EMSA monitors IT operations in an automatic way by means of a monitoring tool (Nagios).

CARD provides the relevant metrics for real-time service operation monitoring in a way that any malfunction, service degradation or downtime can be quickly detected and service restore actions can be undertaken.

CARD provides as a minimum the following metrics:

1. number of Authorization Service requests in the last 15 min
2. number of Authorization Service requests in the last 60 min
3. number of Policy Distribution Service requests in the last 24 hours

Req. 29. CARD meets all the Administration, activity logging and monitoring requirements stated in the section 13.

--- End of Document ---

ABOUT THE EUROPEAN MARITIME SAFETY AGENCY

The European Maritime Safety Agency is one of the European Union's decentralised agencies. Based in Lisbon, the Agency provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long-range identification and tracking of vessels.

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu

EMSA